aws

Benutzer-Leitfaden

AWS Security Hub



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Hub: Benutzer-Leitfaden

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was sind Security Hub und Security Hub CSPM? ... 1
AWS Security Hub ... 2
Features ... 2
Integrationen ... 3
Zugreifen auf Security Hub ... 4
Konzepte ... 4
Kostenschätzer ... 10
Zugriff nach Kontotyp ... 11
Voraussetzungen ... 12
Einrichten des kontoübergreifenden Zugriffs ... 13
Den Kostenschätzer verwenden ... 16
Wichtige Hinweise ... 24
Ähnliche Informationen ... 25
Security Hub aktivieren ... 25
Aktivieren Sie Security Hub für eine AWS Organisation ... 26
Security Hub in einem eigenständigen Konto aktivieren ... 29
Benennung eines delegierten Administrators ... 30
Erstellen der Richtlinie für delegierte Administratoren ... 32
Verwaltung der Konfiguration von Mitgliedskonten ... 33
Einen delegierten Administrator entfernen ... 39
Re-enabling Sicherheits-Hub ... 39
Empfehlungen ... 40
Kontoabdeckung ... 42
Seite zur Kontoabdeckung ... 42
Widget „Sicherheitsabdeckung“ ... 44
Erweiterter Tarif ... 44
Berechtigungen für den erweiterten Tarif ... 45
Registrierung für Partner mit erweitertem Tarif ... 45
Abmeldung von einem Partner ... 46
Cross-Region Aggregation ... 46
Arten von Daten, die aggregiert sind ... 47
Aggregation für Administrator- und Mitgliedskonten ... 49
Automatisierungsregeln und regionsübergreifende Aggregation ... 49
Aggregation aktivieren ... 50

Überprüfung der Aggregationseinstellungen ... 51
Aktualisierung der Aggregationseinstellungen ... 51
Aggregation wird gelöscht ... 52
Integration mit Azure ... 53
Wie AWS Config wird benutzt ... 55
Zusätzliche Informationen ... 55
Voraussetzungen ... 56
Konfiguration von Azure ... 58
Konfigurieren von Security Hub ... 69
Löschen eines Azure-Connectors ... 83
Übersichts-Dashboard ... 84
Überlegungen ... 84
Verfügbare Widgets ... 85
Verfügbare Filter ... 99
Details zu Ressourcen in Security Hub anzeigen ... 101
Format finden: OCSF ... 102
OCSF im Überblick ... 102
Zugehörige Ressourcen ... 103
AWS Erweiterung für OCSF ... 103
Abdeckungserkenntnisse ... 126
Ergebnisse der Netzabdeckung für AWS Security Hub CSPM ... 126
Ergebnisse der Berichterstattung für Amazon GuardDuty ... 127
Ergebnisse der Berichterstattung für Amazon Inspector ... 127
Ergebnisse der Berichterstattung für Amazon Macie ... 128
Ergebnisse der Berichterstattung werden unterdrückt ... 128
KI-Inventar ... 129
Voraussetzungen für die selbst gehostete KI-Erkennung ... 129
Unterstützte KI-Ressourcentypen ... 130
Suchen nach KI-Ressourcen auf der Seite „Ressourcen“ ... 131
Verwenden Sie die KI-Inventarseite ... 131
Überlegungen ... 132
Mit der API auf das KI-Inventar zugreifen ... 133
Ressourcen ... 135
Wie Security Hub auf Kritikalität schließen kann ... 135
Überschreiben der Kritikalität mit einer Automatisierungsregel ... 135
Wie wirkt sich Kritikalität auf den Schweregrad der Expositionsfindung ... 135

Befunde zur Exposition ... 136
Wie funktionieren Expositionsergebnisse ... 136
Bestandteile einer Risikofeststellung ... 137
Klassifizierung des Schweregrads ... 139
Vorteile von Expositionsergebnissen ... 139
Quellen der Feststellungen zur Exposition ... 140
Bewährte Methoden ... 140
Unterstützte Ressourcen ... 141
Unterstützte Eigenschaften ... 142
Generierung von Expositionsergebnissen ... 146
Bestimmung des Schweregrads eines Expositionsergebnisses ... 151
Überprüfung der Ergebnisse zur Exposition ... 153
Diagramm des potenziellen Angriffspfads ... 155
Behebung von Expositionsfeststellungen ... 156
Erkenntnisse zum ungenutzten Zugriff ... 272
So funktioniert die Analyse ungenutzter Zugriffe ... 272
Ungenutzte Typen zur Zugriffsermittlung ... 273
Service-linked Analysator ... 273
Ergebnisse ungenutzter Zugriffe anzeigen ... 274
Ungenutzter Zugriff auf Expositionsergebnisse ... 274
Politische Empfehlungen für ungenutzte Berechtigungen ... 275
Preisgestaltung ... 275
Politische Empfehlungen ... 275
So funktionieren politische Empfehlungen ... 275
Wer kann Empfehlungen generieren ... 276
Lebenszyklus der Empfehlung ... 276
Fehlerfälle ... 277
Verwenden der Konsole ... 277
API-Referenz ... 277
Scannen im Netzwerk ... 278
Unterstützte Ressourcentypen ... 278
Netzwerk-Scannen aktivieren ... 279
So funktioniert das Scannen im Netzwerk ... 280
Ergebnisse von Netzwerk-Scans ... 280
Beweise scannen ... 284
Ressourcen vom Scannen ausschließen ... 284

Unterstützte Anschlüsse ... 285
Multi-cloud Unterstützung ... 285
Verfügbarkeit in Regionen ... 285
Deaktivieren Sie das Scannen im Netzwerk ... 285
Pläne zur Problembehebung ... 286
So erstellt Security Hub Behebungspläne ... 287
Einzelheiten zum Abhilfeplan ... 287
Status des Sanierungsplans ... 288
Anleitung zur Problembehebung ... 288
Behebungspläne anzeigen ... 289
Behebungspläne filtern ... 290
Die Risiken anzeigen, auf die sich ein Plan auswirkt ... 290
Abhilfepläne für ein Risiko anzeigen ... 291
Nachverfolgung der Auswirkungen von Abhilfemaßnahmen auf dem Dashboard ... 291
Automatisierungen ... 291
Automatisierungsregeln ... 292
EventBridge Automatisierungsregeln ... 317
Exportieren von Erkenntnissen ... 326
So funktioniert der Export von Ergebnissen ... 326
Voraussetzungen ... 327
Einen Export erstellen ... 327
Third-party Integrationen ... 3
Jira Cloud ... 328
ServiceNow ... 335
Wichtige KMS-Richtlinien für Ticketing-Integrationen ... 342
Testen von Ticketing-Integrationen ... 346
MCP-App (Vorschau) ... 348
Beispiele für MCP-Apps ... 349
Die wichtigsten Konzepte ... 353
Voraussetzungen ... 354
Den MCP-Server einrichten ... 355
Connector Diagnostics verwenden ... 355
Verfügbare Tools ... 356
Überwachung der Nutzung und der Kosten ... 357
Wer kann auf die Seite „Nutzung“ zugreifen ... 357
Übersicht der Organisations- und Kontokosten ... 358

Funktionsansicht ... 359
Kontoansicht ... 360
Strategien zur Kostenoptimierung ... 361
Zugehörige Ressourcen ... 362
Security Hub deaktivieren ... 362
Security Hub für ein einzelnes Konto deaktivieren ... 362
Security Hub unternehmensweit deaktivieren ... 363
Sicherheit ... 365
Datenschutz ... 366
Identity and Access Management ... 370
Compliance-Validierung ... 405
Ausfallsicherheit ... 405
Sicherheit der Infrastruktur ... 405
VPC-Endpunkte (AWS PrivateLink) ... 406
Protokollieren von API-Aufrufen ... 408
Informationen zum Security Hub finden Sie unter CloudTrail ... 408
Beispiel: Einträge in der Security Hub-Protokolldatei ... 409
AWS Security Hub CSPM ... 413
Vorteile von Security Hub CSPM ... 414
Zugreifen auf Security Hub CSPM ... 415
Zugehörige Services ... 417
Security Hub CSPM — kostenlose Testversion, Nutzung und Preisgestaltung ... 417
Nutzungsdetails anzeigen ... 418
Preisdetails ... 418
Konzepte ... 418
Security Hub CSPM aktivieren ... 425
Überprüfung der erforderlichen Berechtigungen ... 425
Aktivierung von Security Hub CSPM mit der Organisationsintegration ... 425
Manuelles Aktivieren von Security Hub CSPM ... 427
Nächste Schritte: Bestandsmanagement und Integrationen ... 430
Konfiguration AWS Config ... 430
Lokale Konfiguration ... 437
Zentrale Konfiguration ... 438
Verwalten mehrerer Konten ... 490
Konten verwalten mitAWS Organizations ... 491
Manuelles Verwalten von Konten auf Einladung ... 492

Empfehlungen für Umgebungen mit mehreren Konten ... 492
Konten verwalten mit AWS Organizations ... 494
Verwalten von Konten auf Einladung ... 511
Zulässige Aktionen von Administrator- und Mitgliedskonten ... 526
Auswirkung von Kontoaktionen auf Daten ... 533
Aggregation von Daten über Regionen hinweg ... 536
Arten von Daten, die aggregiert sind ... 537
Aggregation für Administrator- und Mitgliedskonten ... 539
Zentrale Konfiguration und Aggregation ... 540
Aggregation aktivieren ... 541
Überprüfung der Aggregationseinstellungen ... 543
Aktualisierung der Aggregationseinstellungen ... 545
Die Aggregation wird beendet ... 547
Standards ... 548
Referenz zu Standards ... 550
Einen Standard aktivieren ... 665
Überprüfung der Einzelheiten eines Standards ... 672
Automatisch aktivierte Standards ausschalten ... 676
Deaktivierung eines Standards ... 678
Kontrollen ... 681
Ansicht „Konsolidierte Steuerelemente“ ... 681
Zusammenfassung der Sicherheitsbewertung für Kontrollen ... 683
Referenz zu Steuerelementen ... 684
Berechtigungen zur Konfiguration von Steuerelementen ... 1676
Steuerelemente aktivieren ... 1677
Deaktivierung der Steuerelemente ... 1686
Sicherheitsüberprüfungen und Ergebnisse ... 1699
Kategorien kontrollieren ... 1777
Überprüfung der Einzelheiten der Kontrollen ... 1781
Steuerelemente zum Filtern und Sortieren ... 1784
Steuerungsparameter ... 1785
Überprüfung und Verwaltung der Kontrollergebnisse ... 1801
Integrationen ... 1829
Überprüfung einer Liste von Integrationen ... 1830
Den Fluss von Erkenntnissen aus einer Integration ermöglichen ... 1832
Deaktivierung des Flusses von Erkenntnissen aus einer Integration ... 1833

Ergebnisse einer Integration anzeigen ... 1834
AWS-Service Integrationen ... 1835
Third-party Integrationen ... 1858
Maßgeschneiderte Produktintegrationen ... 1894
Integration mit Azure ... 1896
Wie AWS Config wird verwendet ... 1897
Arten von Anschlüssen ... 1898
Voraussetzungen ... 1899
Konfiguration von Azure ... 1901
Security Hub CSPM konfigurieren ... 1908
Löschen eines Azure-Connectors ... 1930
Ergebnisse ... 1931
BatchImportFindings um Anbieter zu finden ... 1933
BatchUpdateFindings für Kunden ... 1936
Einzelheiten und Verlauf der Ergebnisse überprüfen ... 1940
Filtern von Ergebnissen ... 1946
Gruppieren der Ergebnisse ... 1948
Den Workflow-Status von Ergebnissen festlegen ... 1949
Senden von Ergebnissen an eine benutzerdefinierte Aktion ... 1953
Suchformat: ASFF ... 1953
Insights ... 2253
Erkenntnisse überprüfen und entsprechend handeln ... 2254
Verwaltete Insights ... 2257
Benutzerdefinierte Insights ... 2268
Automatisierungen ... 2276
Automatisierungsregeln ... 2277
Automatisierte Reaktion und Problembehebung ... 2304
Übersichts-Dashboard ... 2322
Verfügbare Widgets für das Übersichts-Dashboard ... 2323
Das Dashboard filtern ... 2326
Das Dashboard anpassen ... 2329
Regionale Grenzen ... 2330
Cross-Region Einschränkungen bei der Aggregation ... 2330
Verfügbarkeit von Integrationen nach Regionen ... 2330
Verfügbarkeit von Standards nach Regionen ... 2333
Verfügbarkeit von Kontrollen nach Regionen ... 2333

Regionale Grenzwerte für Kontrollen 2333
Ressourcen erstellen mit CloudFormation 2602
Security Hub CSPM undCloudFormationVorlagen 2603
Erfahren Sie mehr überCloudFormation 2604
Ankündigungen abonnieren 2604
Amazon-SNS-Nachrichtenformat 2610
Security Hub CSPM deaktivieren 2611
Sicherheit 2614
Datenschutz 2615
Identity and Access Management 2616
Compliance-Validierung 2654
Ausfallsicherheit 2654
Sicherheit der Infrastruktur 2655
VPC-Endpunkte (AWS PrivateLink) 2655
Protokollieren von API-Aufrufen 2657
Security Hub CSPM-Informationen in CloudTrail 408
Beispiel: Security Hub CSPM-Protokolldateieinträge 409
Taggen von Ressourcen 2661
Grundlagen des Kennzeichnens 2661
Verwenden von Tags in IAM-Richtlinien 2663
Hinzufügen von Tags zu Ressourcen 2664
Tags für Ressourcen bearbeiten 2667
Überprüfung der Tags für Ressourcen 2669
Entfernen von Tags von Ressourcen 2672
Kontingente 2674
Maximale Kontingente 2674
Ratenkontingente 2674
Dokumentverlauf 2675
..... mmdcccii

Was sind Security Hub und Security Hub CSPM?

AWSSecurity Hub und AWS Security Hub CSPM schützen Ihre Cloud-Umgebung. AWS-Services Die Dienste ergänzen sich gegenseitig. Wenn sie zusammen verwendet werden, bieten sie wertvolle Einblicke in den Sicherheitsstatus Ihrer AWS Umgebung.

Security Hub CSPM bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen dabei, Ihre Cloud-Umgebung anhand von Industriestandards und Best Practices zu bewerten. Security Hub bietet ein einheitliches Erlebnis, mit dem Sie kritische Sicherheitsprobleme priorisieren und darauf reagieren können. Die CSPM-Ergebnisse von Security Hub werden automatisch an Security Hub weitergeleitet, wo sie mit Ergebnissen anderer Sicherheitsdienste wie Amazon Inspector korreliert werden, um Risiken zu generieren. Auf diese Weise können Sie die kritischsten Risiken in Ihrer Umgebung identifizieren. Security Hub bietet auch automatisierte Workflow-Funktionen, mit denen Sie die CSPM-Ergebnisse von Security Hub in Ihre betrieblichen Workflows integrieren können.

Als bewährte Methode empfehlen wir, beide Dienste zu aktivieren. Sie können Security Hub CSPM aktivieren, ohne Security Hub zu aktivieren, wenn Ihr Hauptaugenmerk auf der Identifizierung von Fehlkonfigurationen und der Bewertung Ihres Sicherheitsstatus liegt. Wenn Sie Security Hub jedoch aktivieren, ohne Security Hub CSPM zu aktivieren, kann Security Hub die Ergebnisse des Security Hub CSPM nicht verwenden, um Informationen über Risiken und Gefahren in Ihrer Umgebung bereitzustellen. AWS Für ein optimales Erlebnis empfehlen wir, nicht nur Security Hub und Security Hub CSPM zu aktivieren, sondern auch diese anderen Sicherheitsdienste zu aktivieren: Amazon GuardDuty, Amazon Inspector und Amazon Macie.

Einführung in AWS Security Hub

AWS Security Hub ist eine einheitliche Cloud-Sicherheitslösung, die Ihre kritischen Sicherheitsprobleme priorisiert und Ihnen hilft, in großem Umfang darauf zu reagieren. Security Hub erkennt Sicherheitsprobleme, indem es Sicherheitssignale aus mehreren Quellen automatisch korreliert und anreichert. Zu diesen Quellen gehören Statusmanagement, Schwachstellenmanagement (Amazon Inspector), sensible Daten (Amazon Macie) und Bedrohungserkennung (Amazon GuardDuty). Verwenden Sie Security Hub, um aktive Risiken in Ihrer Cloud-Umgebung durch automatisierte Analysen und kontextuelle Einblicke zu priorisieren. Durch intuitive Visualisierungen wandelt Security Hub komplexe Sicherheitssignale in umsetzbare Erkenntnisse um, sodass Sie schnell fundierte Entscheidungen über Ihre Sicherheit treffen können. Security Hub umfasst auch automatisierte Reaktionsworkflows, mit denen Sie Risiken minimieren, die Teamproduktivität verbessern und Betriebsunterbrechungen minimieren können.

Features

Einheitliche Sicherheitslösung

Verschaffen Sie sich durch zentralisiertes Management in einer einheitlichen Cloud-Sicherheitslösung einen umfassenderen Überblick über Ihre gesamte Cloud-Umgebung.

Umsetzbare Einblicke in die Sicherheit

Gewinnen Sie mithilfe fortschrittlicher Analysen umsetzbare Einblicke in die Sicherheit, um mehr über die mit Ihrer Umgebung verbundenen Sicherheitsrisiken zu erfahren.

Verkürzte Reaktionszeiten

Optimieren Sie die Reaktionszeiten mit automatisierten Workflows und einem integrierten Ticketsystem.

Ergebnisse zur Exposition

Security Hub korreliert Ergebnisse von Security Hub CSPM-Kontrollprüfungen, Amazon Inspector und anderen, um Risiken im Zusammenhang AWS-Services mit Ressourcen zu erkennen. AWS

Analyse ungenutzter Zugriffe

Security Hub identifiziert automatisch IAM-Rollen, Benutzer, Zugriffsschlüssel und Berechtigungen, die innerhalb eines 90-tägigen Lookback-Zeitraums nicht verwendet wurden. Wenn Sie Security

Hub aktivieren, erstellt der Dienst einen dienstverknüpften IAM Access Analyzer in Ihrem Konto. Die Ergebnisse ungenutzter Zugriffe helfen Ihnen bei der Implementierung des Zugriffs mit den geringsten Rechten, indem IAM-Prinzipale hervorgehoben werden, die zu viele Zugriffsrechte zugewiesen haben. Für ungenutzte Berechtigungen kann Security Hub Empfehlungen für Richtlinien mit den geringsten Rechten erstellen, die Ihnen eine detaillierte Ersatzrichtlinie aufzeigen.

Die Ergebnisse werden im Open Cybersecurity Schema Framework (OCSF) formatiert

Security Hub generiert Ergebnisse in OCSF und erhält Ergebnisse in OCSF von Security Hub CSPM und anderen: AWS-Services

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Dashboard

Die Security Hub Hub-Konsole bietet einen umfassenden Überblick über Ihre Risiken, Bedrohungen, Sicherheitsvorkehrungen und Ressourcen sowie eine interaktive Visualisierung, das sogenannte Angriffspfaddiagramm, das zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und diese kontrollieren können, die mit einer Sicherheitslücke verknüpft sind.

Integrationen mit Produkten von Drittanbietern

Sie können Ihre Sicherheitslage mit Security Hub Hub-Integrationen verbessern. Wenn Sie beispielsweise Jira Cloud oder verwendenServiceNow ITSM, können Sie diese Funktion verwenden, um Tickets aus Ergebnissen zu erstellen.

Integrationen

Security Hub erhält Ergebnisse aus den folgenden Quellen AWS-Services.

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- IAM Access Analyzer

Zugreifen auf Security Hub

Security Hub ist in den meisten AWS Regionen verfügbar. Eine Liste der Regionen, in denen Security Hub derzeit verfügbar ist, finden Sie unter Security Hub Hub-Endpunkte und Kontingente in der Allgemeine AWS-Referenz. Informationen zur Verwaltung AWS-Regionen für Sie finden Sie im AWS -Kontenverwaltung Referenzhandbuch unter Angeben AWS-Konto, welche Konten für AWS-Regionen Ihr Konto verwendet werden können.

Sie können Security Hub für einzelne Konten oder Konten in Ihrer Organisation aktivieren. In jeder Region können Sie auf eine der folgenden Arten auf Security Hub zugreifen und ihn verwenden:

Security Hub Hub-Konsole

Die Security Hub Hub-Konsole ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. In dieser Konsole können Sie auf Ihr Konto, Ihre Daten und Ressourcen zugreifen.

Security Hub HUB-API

Die Security Hub Hub-API ermöglicht Ihnen programmatischen Zugriff auf Ihr Konto, Ihre Daten und Ressourcen. Sie können HTTPS-Anfragen direkt an Security Hub senden.

AWS CLI

Mit dem AWS CLI können Sie Befehle in der Befehlszeile Ihres Systems ausführen, um Aufgaben auszuführen, und Skripts erstellen, die Aufgaben ausführen. In einigen Fällen AWS CLI kann sie nützlicher sein als die Security Hub Hub-Konsole.

AWS SDKs

AWS SDKs bestehen aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (C++, Go, Java, .NET und Python). Sie bieten programmatischen Zugriff auf Security Hub und andere Anwendungen AWS-Services in Ihrer bevorzugten Sprache und können Ihnen helfen, Aufgaben wie das Verwalten von Fehlern, das Signieren von Anfragen und das Wiederholen von Anfragen zu verwalten.

Security Hub Hub-Konzepte

In Security Hub bauen wir auf gemeinsamen AWS Konzepten und Terminologie auf und verwenden diese zusätzlichen Begriffe.

Account

Das AWS Standardkonto, das Ihre AWS Ressourcen enthält. Melden Sie sich AWS mit Ihrem AWS Konto an, um Security Hub zu aktivieren.

Wenn Ihr Konto registriert ist AWS Organizations, weist Ihre Organisation ein Security Hub-Administratorkonto zu. Dieses Konto kann andere Unternehmenskonten als Mitgliedskonten aktivieren.

Eine Organisation kann nur ein Administratorkonto haben. Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Security Hub unterstützt die folgenden Konten:

- Organisationsverwaltungskonto — ein AWS Konto, das eine AWS Organisation verwaltet.
- Delegiertes Administratorkonto — ein AWS Konto, das die Verwendung eines AWS-Service für eine AWS Organisation verwaltet.
- Mitgliedskonto — ein AWS Konto, das Mitglied einer AWS Organisation ist.
- Eigenständiges Konto — ein AWS Konto ohne AWS Organizations Aktivierung.

Administratorkonto

Bei diesem AWS Kontotyp können Ergebnisse für verknüpfte Mitgliedskonten angezeigt werden.

Dieser AWS Kontotyp wird zu einem Administratorkonto, wenn das Konto von einem Organisationsverwaltungskonto als Security Hub-Administratorkonto festgelegt wird. Das Security Hub-Administratorkonto kann jedes Unternehmenskonto als Mitgliedskonto aktivieren und auch andere Konten als Mitgliedskonten einladen.

Eine Organisation kann nur ein Administratorkonto haben. Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Aggregationsregion

Ein Aggregationsbereich ermöglicht es Ihnen, Sicherheitserkenntnisse aus mehreren Bereichen AWS-Regionen in einem einzigen Fenster anzuzeigen.

In der Aggregationsregion können Sie AWS-Region Ergebnisse einsehen und verwalten. Die Ergebnisse werden in der Aggregationsregion aus verknüpften Regionen aggregiert. Aktualisierte Ergebnisse werden in allen Regionen repliziert.

In der Aggregationsregion enthalten das Dashboard und die Inventarseiten Daten aus allen verknüpften Regionen. Die Automationsseite kann nur verwendet werden, um Automatisierungsregeln in der Aggregationsregion zu definieren. Third-party Ticketing-Integrationen können nur in der Aggregationsregion konfiguriert werden.

Archiviertes Ergebnis

Ein Befund mit dem Status. `ARCHIVED` Diese Ergebnisse deuten darauf hin, dass der Anbieter oder Kunde, der das Ergebnis untersucht, der Ansicht ist, dass das Ergebnis nicht mehr relevant ist.

Finding Provider können die von ihnen erstellten Ergebnisse archivieren. Kunden können alle Ergebnisse, die ihrer Meinung nach nicht mehr relevant sind, mithilfe der BatchUpdateFindingsV2Security Hub Hub-API oder durch Aktualisierung des Status in der Security Hub Hub-Konsole archivieren.

In der Security Hub Hub-Konsole schließen die Standardfiltereinstellungen archivierte Ergebnisse aus Suchlisten und Tabellen aus. Sie können die Filter aktualisieren, um archivierte Ergebnisse einzubeziehen. Wenn Sie Ergebnisse mithilfe des GetFindingsV2-Vorgangs abrufen, ruft der Vorgang sowohl archivierte als auch aktive Ergebnisse ab. Das folgende Beispiel zeigt, wie archivierte Ergebnisse in den Ergebnissen ausgeschlossen werden können.

```
{
    "StringFilters":
    [
        {
            "FieldName": "status",
            "Filter":
            {
                "Value": "Archived",
                "Comparison": "EQUALS"
            }
        }
    ]
}
```

Cross-Region Aggregation

Die Aggregation von Ergebnissen und Ressourcen aus verknüpften Regionen zu einer Aggregationsregion. Sie können alle Ihre Daten aus der Aggregationsregion anzeigen und die Ergebnisse aus der Aggregationsregion aktualisieren.

Delegiertes Administratorkonto

AWS Organizations In kann das delegierte Administratorkonto für einen Dienst die Nutzung eines Dienstes für die Organisation verwalten.

In Security Hub ist das Security Hub-Administratorkonto auch das delegierte Administratorkonto für Security Hub. Wenn das Organisationsverwaltungskonto das Security Hub-Administratorkonto zum ersten Mal festlegt, ruft Security Hub Organizations auf, dieses Konto zum delegierten Administratorkonto zu machen.

Das Organisationsverwaltungskonto muss dann das delegierte Administratorkonto als Security Hub-Administratorkonto in allen Regionen auswählen.

Sicherheitsrisiko

Sicherheitslücken sind umfassendere Schwächen bei Sicherheitskontrollen, Fehlkonfigurationen oder anderen Bereichen, die durch aktive Bedrohungen ausgenutzt werden könnten.

Zu den Risikopositionen gehören beispielsweise:

- Falsch konfigurierte Steuerungsebene für eine Ressource.
- Vorhandensein einer Softwareschwachstelle mit hohem Ausnutzungspotenzial.
- Öffentlich zugängliche Ressource (Netzwerk oder API).

Feststellung der Exposition

Eine Art von Befund, der eine in Ihrer Umgebung vorhandene Exposition beschreibt. Ein Expositionsergebnis umfasst Merkmale und Signale. Ein Signal kann eine oder mehrere Arten von Expositionsmerkmalen enthalten. AWS Security Hub generiert eine Risikofeststellung, wenn Signale von AWS Security Hub CSPM, Amazon Inspector, Amazon GuardDuty, Amazon Macie oder anderen AWS Diensten auf das Vorliegen einer Gefährdung hinweisen. Eine Ressource kann an einer oder mehreren Expositionsfeststellungen beteiligt sein. Wenn eine Ressource keine oder nur unzureichende Expositionsmerkmale aufweist, generiert Security Hub keine Expositionsfeststellung für diese Ressource.

Ein Beispiel für eine Sicherheitslücke ist: Eine EC2-Instance, die über das Internet erreichbar ist und Software-Sicherheitslücken aufweist, die mit hoher Wahrscheinlichkeit ausgenutzt werden können.

Erkenntnis

Der beobachtbare Datensatz einer Sicherheitsprüfung oder sicherheitsrelevanten Erkennung. Security Hub generiert und aktualisiert Ergebnisse durch die Korrelation anderer

Sicherheitsergebnisse. Diese werden als Expositionsergebnisse bezeichnet. Die Ergebnisse können auch aus Integrationen mit anderen Produkten AWS-Services und Produkten von Drittanbietern stammen.

Feststellen von verschluckten Substanzen

Der Import von Ergebnissen in Security Hub. Das Auffinden von Verschluckungsereignissen umfasst sowohl neue Erkenntnisse als auch Aktualisierungen vorhandener Ergebnisse.

Verknüpfte Region

Wenn Sie die regionsübergreifende Aggregation aktivieren, ist eine verknüpfte Region eine Region, die Ergebnisse und Ressourceninventar in der Aggregationsregion zusammenfasst.

In einer verknüpften Region enthalten das Dashboard und die Inventarseiten nur Ergebnisse für diese Region. AWS-Region

Öffnen Sie das Cybersecurity Schema Framework (OCSF)

Das Open Cybersecurity Schema Framework (OCSF) ist eine gemeinsame Open-Source-Initiative von AWS führenden Partnern in der Cybersicherheitsbranche. OCSF bietet ein Standardschema für allgemeine Sicherheitsereignisse, definiert Versionierungskriterien, um die Schemaentwicklung zu erleichtern, und beinhaltet einen Selbstverwaltungsprozess für Hersteller und Nutzer von Sicherheitsprotokollen. Weitere Informationen finden Sie unter OCSF-Ergebnisse in Security Hub.

Mitgliedskonto

Eine AWS-Konto , die einem Administratorkonto die Erlaubnis erteilt hat, ihre Ergebnisse einzusehen und entsprechende Maßnahmen zu ergreifen. Diese Art AWS-Konto wird zu einem Mitgliedskonto, wenn das Security Hub-Administratorkonto sie als Mitgliedskonto aktiviert.

Signal

Ein Befund, der zur Feststellung einer Exposition beiträgt. Ein Signal kann als beitragendes Ergebnis bezeichnet werden. Ein Signal kann von Security Hub, CSPM oder einem anderen AWS Config System wie Amazon AWS-Services Inspector stammen.

Service-linked Konfigurationsrekorder

Ein AWS Config Rekordertyp, der zum Aufzeichnen von Konfigurationsdaten auf dienstspezifischen Ressourcen verwendet wird. Security Hub verwendet diese Rekorder in einem ereignisgesteuerten Ansatz, um Ressourcenkonfigurationselemente für die Risikoanalyse, den Umfang, die Berichterstattung über den Ressourcenbestand und die Bewertung der Statusmanagementkontrolle abzurufen. Diese Funktion wird allen Security Hub-Kunden im

Rahmen der Preise für den Essential-Plan zur Verfügung gestellt. Nachdem Sie Security Hub aktiviert haben, werden die folgenden serviceverknüpften Konfigurationsrekorder in Ihrem Konto erstellt:

- In jeder Gruppe wird AWS-Konto ein mit dem Dienst verknüpfter Konfigurationsrekorder mit dem Namen `AWSConfigurationRecorderForSecurityHubAssets` erstellt. AWS-Region
- Für globale Ressourcentypen `AWSConfigurationRecorderForSecurityHubAssetsGlobal` wird ein zusätzlicher serviceverknüpfter Konfigurationsrekorder mit dem Namen AWS-Region us-east-1 erstellt.
- Wenn Security Hub und Security Hub CSPM beide in einem AWS-Konto und aktiviert sind AWS-Region, wird ein dienstverknüpfter Konfigurationsrekorder mit dem Namen `AWSConfigurationRecorderForSecurityHubCSPM` erstellt.

Weitere Informationen finden Sie unter Überlegungen zu serviceverknüpften Konfigurationsrekordern und Aufzeichnen regionaler und globaler Ressourcen.

Service-linked Analysator

Ein IAM Access Analyzer, den Security Hub in Ihrem Namen erstellt und verwaltet. Wenn Sie Security Hub aktivieren, erstellt es automatisch einen servicebezogenen Analyzer für ungenutzten Zugriff, um IAM-Rollen, Benutzer, Zugriffsschlüssel und Berechtigungen zu identifizieren, die innerhalb eines 90-tägigen Lookback-Zeitraums nicht verwendet wurden. Der Analyzer wird in USA East (Nord-Virginia) ausgeführt, da IAM ein globaler Dienst ist. Security Hub repliziert ungenutzte Zugriffsergebnisse in alle Regionen, in denen Sie Security Hub aktiviert haben. Sie müssen IAM Access Analyzer nicht separat aktivieren oder zusätzliche Maßnahmen ergreifen. Diese Funktion wird allen Security Hub-Kunden im Rahmen der Preise für den Essential-Plan zur Verfügung gestellt. Sie können den Service Linked Analyzer in der IAM Access Analyzer-Konsole anzeigen, aber Sie können ihn nicht ändern oder löschen, solange Security Hub aktiviert ist. Security Hub löscht den Analyzer, wenn Sie den Dienst in allen Regionen eines AWS-Konto deaktivieren. Weitere Informationen finden Sie unter the section called “Erkenntnisse zum ungenutzten Zugriff”.

Merkmal

Eine Sicherheitsabweichung, die zu einer Risikofeststellung führt. Zu den Merkmalstypen gehören Vermutbarkeit, Fehlkonfiguration, Erreichbarkeit, sensible Daten und Sicherheitslücke. Ein Merkmal ist mit einem Signal verknüpft, und ein Signal kann mehrere Merkmale enthalten. Ein Security Hub CSPM-Steuerelement weist beispielsweise darauf hin, dass eine vom Kunden verwaltete Richtlinie eine administrative Zugriffskontrolle ermöglicht. Dieses Signal enthält ein Merkmal einer Fehlkonfiguration.

Erkenntnis zum ungenutzten Zugriff

Ein Ergebnis, das eine IAM-Rolle, einen Benutzer, einen Zugriffsschlüssel oder eine Reihe von Berechtigungen identifiziert, die innerhalb eines 90-tägigen Lookback-Zeitraums nicht verwendet wurden. Security Hub generiert ungenutzte Zugriffsergebnisse mithilfe eines serviceverknüpften IAM Access Analyzer. Es gibt vier Arten von Ergebnissen bei ungenutztem Zugriff: ungenutzte IAM-Rollen, ungenutzte IAM-Benutzerzugriffsschlüssel, ungenutzte IAM-Benutzerkennwörter und ungenutzte Berechtigungen.

AWS Kostenschätzer für Security Hub

Der Security Hub-Kostenschätzer ist eine Konsolenfunktion, die Schätzungen der Security Hub-Funktionen in Ihrer AWS gesamten Umgebung liefert. Der Kostenschätzer zeigt Ihnen, wie hoch Ihre individuellen Servicekosten für AWS Security Hub CSPM, Amazon Inspector und Amazon sind GuardDuty und wie hoch Ihre geschätzten Kosten bei Security Hub mit den vereinfachten Preisplänen von Security Hub wären. Sie können die geschätzte Nutzung und die Anzahl der Ressourcen an Ihre AWS Nutzung anpassen, um die Genauigkeit Ihrer Schätzung zu erhöhen. Der Kostenschätzer ist in allen Regionen verfügbar, in denen Security Hub verfügbar ist.

Der Kostenschätzer schätzt die monatlichen Kosten für Sicherheitsfunktionen anhand von zwei Preismodellen:

- Preise für individuelle Services — Zahlen Sie für jede Sicherheitsfunktion separat (GuardDutyAmazon Inspector, Security Hub CSPM).
- Vereinfachte Preise für Security Hub — Einheitliche Preisgestaltung für 3 Preispläne, Essentials-Paket mit Preisen pro Ressource, Bedrohungsanalysen mit Preisen pro Ereignis und pro GB für Protokolle und Lambda Code Scanning mit Preisen pro Ressource.

Der Schätzer verwendet Daten, sofern verfügbar. AWS Cost Explorer Wenn die Cost Explorer-Daten nicht verfügbar sind, können Sie die Nutzungsdaten manuell eingeben. Kostenschätzungen basieren auf beobachteten und vom Benutzer bereitgestellten Nutzungs- und öffentlichen Preisinformationen. Die Schätzungen spiegeln möglicherweise nicht die Rabatte für Unternehmen wider.

Zu den wichtigsten Vorteilen des Kostenschätzers gehören:

- Sehen Sie, wie sich die Kosten bei einheitlicher Preisgestaltung bei Aktivierung von Security Hub mit den Kosten für einen einzelnen Service ohne Aktivierung von Security Hub vergleichen lassen

- Schätzen Sie die Kosten ab, bevor Sie Funktionen aktivieren
- Passen Sie die Nutzungsparameter an, um verschiedene Szenarien zu modellieren
- Exportieren Sie Schätzungen als PDF zur Überprüfung durch die Stakeholder

Zugriff nach Kontotyp

> **Note**
>
> Für delegierte Administrator- und Mitgliedskonten wird der Kostenschätzer standardmäßig im Bearbeitungsmodus geöffnet, sodass Sie sofort Nutzungsdaten eingeben können. Verwaltungskonten und eigenständige Konten werden im Anzeigemodus geöffnet, wenn Cost Explorer-Daten verfügbar sind.

Diese Funktion ruft automatisch Informationen zur tatsächlichen Nutzung in der Vergangenheit ab, um die Kosten für bestimmte Kontotypen abzuschätzen. In der folgenden Tabelle finden Sie Einzelheiten zu den einzelnen Kontotypen und zu den Daten, die für jeden Kontotyp verfügbar sind.

Zugriffsberechtigungen nach Kontotyp

Account-Typ	Cost Explorer-Daten	Dateneingabe	Scope
Verwaltungskonto (MA)	Auto-populated	Manuelles Übersteuern möglich	Organization-wide
Delegierter Administrator (DA)	Auto-popu lated über eine kontoüber greifende Rolle*	Manuelles Überschreiben möglich	Organization-wide
Mitgliedskonto	Auto-popu lated über eine kontoüber greifende Rolle*	Manuelles Überschreiben möglich	Organization-wide
Eigenständiges Konto (SA)	Auto-populated	Manuelles Überschreiben verfügbar	Einzelkonto

* Erfordert eine kontoübergreifende IAM-Rollenkonfiguration im Verwaltungskonto. Siehe Einrichten des kontoübergreifenden Zugriffs Abschnitt unten.

Voraussetzungen

Erforderliche IAM-Berechtigungen

Um alle Funktionen des Kostenschätzers nutzen zu können, muss Ihr IAM-Principal über die folgenden Berechtigungen verfügen:

Erforderliche IAM-Berechtigungen für Cost Estimator

API-Operation	Service	Zweck
`ce:GetCostAndUsage`	AWS Cost Explorer	Rufen Sie historische Nutzungs- und Kostendaten ab
`pricing:GetProducts`	AWS Preisgestaltung	Aktuelle Tarife abrufen
`organizations:ListAccounts`	AWS Organisationen	Zählen Sie Konten in der Organisation
`organizations:DescribeOrganization`	AWS Organisationen	Ermitteln Sie den Kontotyp
`securityhub:ListOrganizationAdminAccounts`	Sicherheits-Hub	Admin-Konten der Organisation auflisten
`iam:GetRole`	IAM	Prüfen Sie das Vorhandensein kontoübergreifender Rollen (nur Verwaltungskonto) *
`sts:AssumeRole`	IAM	Nehmen Sie die kontoübergreifende Rolle an (nur delegiertes administrator/ Member Konto) **

* Nur für Benutzer des Verwaltungskontos erforderlich, um den kontoübergreifenden Rollenstatus zu überprüfen.

** Nur für Konten delegierter Administratoren und Organisationsmitglieder mit kontoübergreifendem Zugriff erforderlich.

Zusätzliche Anforderungen

Cost Explorer

Muss für die automatische Datenauffüllung aktiviert sein (24-stündige Verarbeitungsverzögerung nach der Aktivierung).

Einrichten des kontoübergreifenden Zugriffs

Delegierte Administrator- und Mitgliedskonten können vom Verwaltungskonto aus auf unternehmensweite AWS Cost Explorer Daten zugreifen, indem sie eine kontoübergreifende IAM-Rolle konfigurieren. Diese Konfiguration ermöglicht es diesen Konten, die tatsächlichen Nutzungsdaten einzusehen, ohne zum Verwaltungskonto wechseln zu müssen.

Voraussetzungen

Vor der Einrichtung des kontoübergreifenden Zugriffs für den Kostenschätzer sind die folgenden Elemente und Informationen erforderlich:

- Das Verwaltungskonto muss AWS Cost Explorer aktiviert sein.
- IAM-Berechtigungen zum Erstellen von Rollen im Verwaltungskonto.
- Kenntnis des delegierten Administrators oder der Mitgliedskonto-ID, dem der kontoübergreifende Zugriff gewährt wird.

Einrichtungsschritte

Der Kostenschätzer bietet Anleitungen zur Einrichtung direkt in der Konsole. Um auf die Anweisungen zuzugreifen, navigieren Sie zur Seite mit dem Kostenvoranschlag unter https://console.aws.amazon.com/securityhub/v2/home #/costEstimator in Ihrem Unternehmensverwaltungskonto. Suchen Sie den Bereich „Cross-account Zugriff“ und folgen Sie den Schritten, die zur Einrichtung der kontoübergreifenden Rolle beschrieben werden.

Rollenkonfiguration

Für den kontoübergreifenden Zugriff für den Kostenschätzer ist die Einrichtung einer IAM-Rolle mit einer Vertrauensrichtlinie und einer Berechtigungsrichtlinie erforderlich. Die kontoübergreifende Rolle muss im Verwaltungskonto mit der folgenden Konfiguration erstellt werden:

Rollenname (genauer Name erforderlich) — AwsSecurityHubCostEstimatorCrossAccountRole

Empfohlene Vertrauensrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::{ACCOUNT_ID}:role/{ROLE_NAME}"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte im Richtlinienbeispiel ersetzen:

- *{ACCOUNT_ID}*Ersetzen Sie es durch die ID des delegierten Administrators oder Mitgliedskontos, für das Sie kontoübergreifenden Zugriff gewähren.
- *{ROLE_NAME}*Ersetzen Sie den Namen der IAM-Rolle im delegierten Administrator- oder Mitgliedskonto, für das Sie Zugriff gewähren.

Empfohlene Berechtigungsrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ce:GetCostAndUsage",
            "Resource": "*"
        }
```

```
    ]
}
```

> **Note**
>
> Die Vertrauensrichtlinie schränkt den Zugriff auf ein bestimmtes Konto und eine bestimmte Rolle ein. Nur der angegebene IAM-Principal kann diese Rolle übernehmen, wodurch unbefugter Zugriff verhindert wird.

Verifizierung

Nachdem Sie die Rolle im Verwaltungskonto erstellt haben, überprüfen Sie anhand der folgenden Schritte, ob das Setup funktioniert.

1. Melden Sie sich beim delegierten Administrator- oder Mitgliedskonto an.
2. Navigieren Sie unter #/costEstimator zum Security Hub-Kostenschätzer https://console.aws.amazon.com/securityhub/v2/home
3. Die Seite sollte automatisch:
    a. Ermitteln Sie das Verwaltungskonto in Ihrer Organisation.
    b. Übernehmen Sie die kontoübergreifende Rolle.
    c. Laden Sie Cost Explorer-Daten mit unternehmensweiter Nutzung.

Bei Erfolg werden die tatsächlichen Nutzungsdaten anstelle der manuellen Eingabefelder angezeigt.

Fehlerbehebung

In diesem Abschnitt werden häufig auftretende Probleme und Lösungen behandelt, die bei der Einrichtung des kontoübergreifenden Zugriffs auftreten können.

Organisatorische Nutzungsdaten sind für dieses Konto nicht verfügbar

Diese Warnung weist darauf hin, dass auf die kontoübergreifende Rolle nicht zugegriffen werden kann. Mögliche Ursachen für diese Warnung sind:

1. Rolle existiert nicht: Das Verwaltungskonto hat die Rolle noch nicht erstellt.

- Lösung: Wenden Sie sich an den Administrator Ihres Verwaltungskontos, um die Rolle mithilfe der Einrichtungsanleitung zu erstellen.

2. Rollennamen stimmen nicht überein: Der Rollenname stimmt nicht exakt überein.

   - Lösung: Stellen Sie sicher, dass der Rollenname lautet`AwsSecurityHubCostEstimatorCrossAccountRole`.

3. Falsche Vertrauensrichtlinie: Die Vertrauensrichtlinie lässt nicht zu, dass Ihr Konto die Rolle übernimmt.

   - Lösung: Stellen Sie sicher, dass die Vertrauensrichtlinie Ihre Konto-ID und Ihren Rollennamen enthält.

4. Fehlende AssumeRole Genehmigung: Ihr IAM-Principal fehlt`sts:AssumeRole`.

   - Lösung: Wenden Sie sich an Ihren Administrator, um die `sts:AssumeRole` Berechtigung hinzuzufügen.

Um detaillierte Anweisungen zur Einrichtung anzuzeigen: Wählen Sie „Anweisungen in der Warnung anzeigen“, um ein Fenster mit schrittweisen Anleitungen und Richtlinienvorlagen zu öffnen.

Problemumgehung: Sie können den Kostenschätzer weiterhin verwenden, indem Sie die Nutzungswerte im Bearbeitungsmodus manuell eingeben.

Den Kostenschätzer verwenden

Zugriff auf den Kostenschätzer

So greifen Sie über die Security Hub-Landingpage auf den Kostenschätzer zu

1. Melden Sie sich mit Ihren Anmeldedaten für die AWS Unternehmensleitung oder das AWS Konto eines delegierten Administrators bei Ihrem Konto an. Öffnen Sie die Security Hub-Konsole in der Region us-east-1 unter. https://console.aws.amazon.com/securityhub/v2/home
2. Suchen Sie auf der Startseite nach der Preisübersicht.
3. Wählen Sie Kosten schätzen aus.

Um während der Aktivierungs- und Konfigurationsschritte von Security Hub auf den Kostenschätzer zuzugreifen

1. Die Preise finden Sie auf der neuen Security Hub-Karte in der Onboarding-Oberfläche.
2. Wählen Sie Kostenvoranschläge anzeigen aus.

Um von der Amazon Inspector- oder Security Hub-CSPM-Konsole aus GuardDuty auf den Kostenschätzer zuzugreifen

1. Navigieren Sie zum Service-Dashboard oder zur Übersichtsseite.
2. Wählen Sie auf der Karte mit den Preisinformationen die Option Preise vergleichen aus.

Grundlegendes zur Benutzeroberfläche des Kostenschätzers

Layout der Seite

Die Seite mit dem Kostenvoranschlag besteht aus drei Hauptabschnitten:

- Abschnitt „Überblick“ — Erläutert die Vorteile eines einheitlichen Sicherheitsmanagements und der Kostenoptimierung.
- Preisinformationen — Erweiterbares Panel mit Funktionskategorien und Preisstufen.
- Preisvergleichstabelle — Side-by-side Kostenvergleich mit Leistungsdetails.

Vergleichstabelle der Preise

Der Tabellenkopf enthält view/edit Modussteuerungen und eine Reset-Option. In der Tabelle werden die Kosten in zwei Spalten angezeigt:

- Einzelne Dienste — Aktuelle oder geschätzte Kosten für separate Sicherheitsdienste.
- Security Hub — Geschätzte Kosten unter Verwendung eines vereinfachten Preismodells.

Preisregion

In der ersten Spalte werden Informationen zum Preiskontext angezeigt, einschließlich eines Hinweises, dass Schätzungen die US-East-1-Preisgestaltung für Berechnungen verwenden. Ein Symbol weist darauf hin, dass Unternehmensrabatte nicht in den Schätzungen enthalten sind.

Kostenvoranschläge anzeigen

Wenn Sie den Kostenschätzer verwenden, können Sie Schätzungen anzeigen, bearbeiten, zurücksetzen und exportieren.

Der Kostenschätzer wird standardmäßig im Anzeigemodus geöffnet.

Um Kostenschätzungen anzuzeigen

1. Greifen Sie mit einer der unter beschriebenen Methoden auf den Kostenschätzer zuZugriff auf den Kostenschätzer.
2. Überprüfen Sie die monatlichen Gesamtkosten in der Übersichtszeile.
3. Prüfen Sie die Funktionsgruppen und ihre detaillierten Kostenaufschlüsselungen.
4. Wählen Sie die Namen der Funktionen, um die Beschreibungen in einem Popover anzuzeigen.

Datenquellen im Anzeigemodus

Der Schätzer zeigt Daten aus mehreren Quellen an, die durch Beschriftungen gekennzeichnet sind:

- Standard — Daten von AWS Cost Explorer (letzte 30 Tage).
- $-/Monat — Kostendaten nicht verfügbar (werden angezeigt, wenn der Cost Explorer-Zugriff nicht verfügbar ist).
- Benutzerdefinierte Nutzung — User-entered Werte.
- Nicht aktiviert — Zeigt an, wenn Cost Explorer-Berechtigungen nicht vorhanden sind.

Account-specific Verhalten

Im Folgenden wird beschrieben, wie der Kostenschätzer für verschiedene Typen, Konten und Konfigurationen funktioniert.

Delegierte Administrator- und Mitgliedskonten

Wenn der kontoübergreifende Zugriff konfiguriert ist:

- Cost Explorer-Daten sind unternehmensweit verfügbar.
- Wird standardmäßig im Anzeigemodus geöffnet (wie beim Verwaltungskonto). Sie können in den Bearbeitungsmodus wechseln, um Schätzungen zu ändern.

Ohne konfigurierten kontoübergreifenden Zugriff:

- Es wird eine Warnung angezeigt: „Organisatorische Nutzungsdaten sind für dieses Konto nicht verfügbar“.
- Wird standardmäßig im Bearbeitungsmodus für die manuelle Eingabe geöffnet.
- Wählen Sie in der Warnung Anweisungen anzeigen, um Anleitungen zur Einrichtung zu erhalten.

Verwaltungskonto

Wenn die kontoübergreifende Rolle erstellt wurde:

- Der Abschnitt „Cross-account Zugriff“ zeigt den konfigurierten Status.
- Zeigt empfohlene Richtlinien zur Überprüfung an.
- Stellt einen Link zur Anzeige der Rolle in der IAM-Konsole bereit.

Ohne dass eine kontoübergreifende Rolle erstellt wurde:

- Im Abschnitt „Cross-account Zugriff“ wird eine Anleitung zur Einrichtung angezeigt.
- Enthält schrittweise Anleitungen mit vorab ausgefüllten Richtlinien.
- Direkter Link zur IAM-Konsole für die Rollenerstellung.

Der Rollenstatus konnte nicht überprüft werden:

- Wenn keine Anrufberechtigung besteht`iam:GetRole`, kann die Konsole nicht feststellen, ob Sie die erforderliche Rolle erstellt haben.
- Zeigt „Überprüfung nicht möglich“ mit der entsprechenden Fehlermeldung an.

Eigenständiges Konto

Ohne dass eine kontoübergreifende Rolle erstellt wurde:

- Keine Änderungen am bestehenden Verhalten.
- Cost Explorer-Daten sind verfügbar, wenn sie aktiviert sind.
- Wird standardmäßig im Anzeigemodus geöffnet.

Nutzungswerte bearbeiten

Im Bearbeitungsmodus können Sie Dimensionswerte ändern und sich Kostenaktualisierungen in Echtzeit anzeigen lassen.

Um Nutzungswerte zu bearbeiten

1. Wählen Sie im Tabellenkopf Bearbeiten.
2. Geben Sie Werte in die Dimensionseingabefelder ein.
3. Lassen Sie sich die aktualisierten Kosten automatisch anzeigen.
4. Wählen Sie Ansicht, um zum Anzeigemodus zurückzukehren.

> **Important**
>
> - Änderungen werden nicht gespeichert, wenn Sie die Seite mit dem Kostenvoranschlag verlassen
> - Bei geänderten Kostenvoranschlägen wird der Preis US-East-1 (Nord-Virginia) verwendet. Rabatte für Unternehmen sind nicht enthalten
> - Bei der Bearbeitung im Modus „Nur aktuelle Kosten anzeigen“ wird automatisch in den Schätzmodus zurückgeschaltet

Der Schätzer wird zurückgesetzt

Diese Aktion löscht alle benutzerdefinierten Werte und lädt die Standarddaten aus dem Cost Explorer neu.

Um alle Werte auf die Standardwerte zurückzusetzen

1. Wählen Sie im Tabellenkopf die Option Zurücksetzen.
2. Wählen Sie im Bestätigungsdialog Reset.

Exportieren von Schätzungen

Während Sie sich im Kostenschätzer befinden, können die Daten für Ihre Schätzung in eine PDF-Datei exportiert werden.

Um Kostenvoranschläge zu exportieren

1. Stellen Sie sicher, dass Sie sich im Anzeigemodus befinden.
2. Wählen Sie im Seitenkopf die Option PDF herunterladen.

Das PDF wird automatisch mit dem Dateinamen heruntergeladen:`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

Fehlerbehebung

In diesem Abschnitt werden häufig auftretende Probleme und Lösungen behandelt, die bei der Verwendung des Kostenschätzers auftreten können

Keine Cost Explorer-Daten verfügbar

Problem

In der Warnung wird angezeigt, dass für Ihr Konto keine Kostendaten verfügbar sind.

Lösungen nach Kontotyp

Die Lösung hängt von Ihrem Kontotyp ab:

Lösungen für fehlende Cost Explorer-Daten

Account-Typ	Lösung
Verwaltungskonto	Aktivieren Sie Cost Explorer und warten Sie 24 Stunden auf die Datenverarbeitung
Delegierter Administrator	Wenden Sie sich an den Administrator des Verwaltungskontos, um Zugriff zu beantragen
Mitgliedskonto	Wenden Sie sich an das Verwaltungskonto oder den delegierten Administrator, um Zugriff zu erhalten
Eigenständiges Konto	Aktivieren Sie Cost Explorer und warten Sie 24 Stunden auf die Datenverarbeitung

Workaround

Geben Sie benutzerdefinierte Werte im Bearbeitungsmodus ein.

Cross-account Zugriff funktioniert nicht

Problem

Beim delegierten Administrator- oder Mitgliedskonto wird die Warnung „Für dieses Konto sind keine organisatorischen Nutzungsdaten verfügbar“ angezeigt.

Informieren Sie sich über die folgenden häufigen Ursachen und deren Lösungen:

Cross-account Die Rolle ist im Verwaltungskonto nicht vorhanden

Wenden Sie sich an den Administrator des Verwaltungskontos, um die Rolle zu erstellen. Der Kostenschätzer bietet Anleitungen zur Einrichtung für Benutzer des Verwaltungskontos.

Der Rollenname stimmt nicht exakt überein

Erforderlicher Rollenname:`AwsSecurityHubCostEstimatorCrossAccountRole`. Stellen Sie sicher, dass der Rollenname in der IAM-Konsole exakt übereinstimmt (Groß- und Kleinschreibung beachten).

Die Vertrauensrichtlinie lässt Ihr Konto nicht zu

Stellen Sie sicher, dass das Prinzip der Vertrauensrichtlinie Ihre Konto-ID und Ihren Rollennamen enthält. Format:`arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`.

Fehlende AssumeRole Erlaubnis

Stellen Sie sicher, dass Ihr IAM-Principal die `sts:AssumeRole` Erlaubnis hat. Wenden Sie sich an Ihren AWS Administrator, um diese Berechtigung hinzuzufügen.

Workaround:

Geben Sie im Bearbeitungsmodus benutzerdefinierte Werte ein, um die Kosten ohne Cost Explorer-Daten manuell zu schätzen.

Erhalten Sie detaillierte Anweisungen

- Wählen Sie in der Warnung Anweisungen anzeigen aus, um ein Modal zu öffnen mit:
  - Step-by-step Anleitung zur Einrichtung
  - Pre-populated Vorlagen für Richtlinien
  - Tipps zur Problembehandlung, die speziell auf Ihren Fehler zugeschnitten sind

Fehler bei der Genehmigung

Problem

Fehler „Zugriff verweigert“ für bestimmte API-Operationen.

Um Berechtigungsfehler zu beheben

1. Notieren Sie sich den verweigerten Vorgang anhand der Fehlermeldung (z. B.`ce:GetCostAndUsage`).
2. Wählen Sie Kopieren, um die Fehlerdetails zu kopieren.
3. Senden Sie die Fehlerdetails an Ihren AWS Administrator.
4. Fordern Sie die erforderlichen IAM-Berechtigungen an, die unter aufgeführt sind. Erforderliche IAM-Berechtigungen

> **Note**
>
> Sie können den Bearbeitungsmodus weiterhin verwenden, um manuelle Werte einzugeben, wenn Berechtigungen fehlen, es sei denn, der Zugriff auf die Pricing-API wird verweigert (verhindert alle Kostenschätzungen).

Für die Funktion wird „Nicht aktiviert“ angezeigt

Problem

Für die Funktion wird der Status „Nicht aktiviert“ angezeigt.

Erklärung

Dieser Status wird angezeigt, wenn Sie Zugriff auf den Cost Explorer haben, die Funktion jedoch derzeit nicht aktiv ist. Wenn Sie stattdessen $-/mo sehen, bedeutet dies, dass Cost Explorer-Daten für Ihren Kontotyp nicht verfügbar sind.

Um Kostenvoranschläge anzuzeigen

1. Wählen Sie Bearbeiten, um den Bearbeitungsmodus aufzurufen.
2. Geben Sie Dimensionswerte für die Fähigkeit ein.
3. Zeigt aktualisierte Kostenschätzungen an.

Für die Funktion wird „Nicht zutreffend“ angezeigt

Problem

Für die Funktion wird in der Spalte „Einzelne Dienste“ der Wert „Nicht zutreffend“ angezeigt.

Erklärung

Diese Funktion ist nur im Rahmen der vereinfachten Preisgestaltung von Security Hub verfügbar, nicht als eigenständiger Service.

Die geänderten Kosten entsprechen nicht dem Cost Explorer

Problem

Die bearbeiteten Kosten unterscheiden sich von den ursprünglichen Cost Explorer-Werten.

Erklärung

Bei den geänderten Schätzungen werden die Preise für US-East-1 (Nord-Virginia) verwendet, Unternehmensrabatte sind nicht enthalten. Die Daten von Cost Explorer spiegeln die tatsächlichen Kosten mit den geltenden Rabatten wider.

Wichtige Hinweise

- Die Schätzungen basieren auf der beobachteten und vom Benutzer bereitgestellten Nutzung sowie auf öffentlichen Preisinformationen. Die tatsächlichen Kosten können je nach Nutzungsmustern und Unternehmensvereinbarungen variieren
- Rückblick auf 30 Tage — Die Daten von Cost Explorer spiegeln die Nutzung der letzten 30 Tage wider
- Preisregion — Bei allen Schätzungen werden die Tarife US-East-1 (Nord-Virginia) verwendet
- Keine Auswirkung auf die Einstellungen — Änderungen im Kalkulator wirken sich nicht auf Ihre aktuellen Security Hub- oder Servicekonfigurationen aus
- Rabatte für Unternehmen — Geänderte Schätzungen beinhalten keine Rabatte für Unternehmen. Nur die Daten von Cost Explorer geben die tatsächlich ermäßigten Kosten wieder
- Datenaktualisierung — Die Daten von Cost Explorer werden täglich aktualisiert. Aktualisieren Sie die Seite, um die neuesten Daten zu sehen

Ähnliche Informationen

- AWS Preisgestaltung für Security Hub
- AWS Cost Explorer-Benutzerhandbuch
- AWS Referenz zur Preisfindungs-API
- Security Hub aktivieren

Security Hub aktivieren

Sie können Security Hub für jeden aktivieren AWS-Konto. In diesem Abschnitt der Dokumentation werden alle Schritte beschrieben, die erforderlich sind, um Security Hub für eine AWS Organisation oder ein eigenständiges Konto zu aktivieren.

> **Important**
>
> Wenn Sie AWS Security Hub aktivieren, verwendet Security Hub die verfügbaren Daten (einschließlich Ergebnisse, Konfigurationsdaten, Softwareinventar und andere Daten aus Ihrer AWS Umgebung), um die von Ihnen aktivierten Funktionen zu aktivieren. Wenn wir bestehende Funktionen erweitern oder neue hinzufügen, kann Security Hub auf zusätzliche Daten zurückgreifen, die sich bereits in seiner Reichweite befinden, um ein besseres Erlebnis zu bieten, z. B. eine genauere Bewertung der realen Auswirkungen von Gefahren in Ihrer Umgebung, ohne zusätzliche Kosten. Sie können Ihre Integrationen und aktivierten Funktionen jederzeit verwalten. Einzelheiten finden Sie in der Security Hub Hub-Dokumentation oder wenden Sie sich bei Fragen an Ihr AWS Account-Team oder den AWS Support.

Eine kurze Demonstration der Aktivierung von Security Hub finden Sie im folgenden Video: Security Hub Onboarding Walkthrough and Demo.

Aktivieren Sie Security Hub für eine AWS Organisation

Dieser Abschnitt umfasst drei Schritte:

- In Schritt 1 bestimmt das AWS Organisationsverwaltungskonto einen delegierten Administrator für das AWS Unternehmen, erstellt die Richtlinie für delegierte Administratoren und aktiviert optional Security Hub für sein eigenes Konto.
- In Schritt 2 aktiviert der delegierte Administrator der Organisation Security Hub für sein eigenes Konto.
- In Schritt 3 konfiguriert der delegierte Administrator der Organisation alle Mitgliedskonten in der Organisation für Security Hub und andere unterstützte Sicherheitsdienste.

Schritt 1. Delegieren eines Administratorkontos und optionale Aktivierung von Security Hub im AWS Verwaltungskonto der Organisation

> **Note**
>
> Führen Sie diesen Schritt in einer Region des Organisationsverwaltungskontos aus.

Bei der Zuweisung des delegierten Administratorkontos für Security Hub hängt das Konto, das Sie für Ihren delegierten Administrator auswählen können, davon ab, wie Sie einen delegierten Administrator für Security Hub CSPM konfiguriert haben. Wenn Sie einen delegierten Administrator für Security Hub CSPM konfiguriert haben und dieses Konto nicht das Organisationsverwaltungskonto ist, wird dieses Konto automatisch als delegierter Security Hub-Administrator eingerichtet und es kann kein anderes Konto ausgewählt werden. Wenn das delegierte Administratorkonto für Security Hub CSPM als Organisationsverwaltungskonto oder überhaupt nicht eingerichtet ist, können Sie wählen, welches Konto als Ihr delegiertes Security Hub-Administratorkonto zugewiesen werden soll, mit Ausnahme des Organisationsverwaltungskontos.

Informationen zur Benennung eines delegierten Administrators in Security Hub finden Sie unter Benennen eines delegierten Administratorkontos in Security Hub. Informationen zum Erstellen der delegierten Administratorrichtlinie in Security Hub finden Sie unter Delegierte Administratorrichtlinie in Security Hub erstellen.

So ernennen Sie einen Administrator für Security Hub

1. Melden Sie sich mit den Anmeldedaten Ihres AWS AWS Organisationsverwaltungskontos bei Ihrem Konto an. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie auf der Security Hub-Startseite Security Hub und dann Erste Schritte aus.
3. Wählen Sie im Bereich Delegierter Administrator ein Administratorkonto auf der Grundlage der bereitgestellten Optionen aus. Es hat sich bewährt, für alle Sicherheitsdienste denselben delegierten Administrator zu verwenden, um eine konsistente Verwaltung zu gewährleisten.
4. Aktivieren Sie das Kontrollkästchen Vertrauenswürdiger Zugriff. Wenn Sie diese Option auswählen, kann Ihr delegiertes Administratorkonto bestimmte Funktionen, wie z. B. den GuardDuty Malware-Schutz, für Mitgliedskonten konfigurieren. Wenn Sie diese Option deaktivieren, kann Security Hub diese Funktionen nicht in Ihrem Namen aktivieren und Sie müssen sie direkt über den Dienst aktivieren, mit dem die Funktion verknüpft ist.

5. (Optional) Wählen Sie für die Kontoaktivierung das Kästchen aus, um Security Hub für Ihr AWS Konto zu aktivieren.
6. Wählen Sie für die Richtlinie für delegierte Administratoren eine der folgenden Optionen, um die Richtlinienerklärung hinzuzufügen.

   a. (Option 1) Wählen Sie Für mich aktualisieren aus. Aktivieren Sie das Kästchen unter der Richtlinienerklärung, um zu bestätigen, dass Security Hub automatisch eine Delegierungsrichtlinie erstellt, die dem delegierten Administrator alle erforderlichen Rechte gewährt.

   b. (Option 2) Wählen Sie Ich möchte das manuell anhängen. Wählen Sie Kopieren und anhängen. Wählen Sie in der AWS Organizations Konsole unter Delegierter Administrator für AWS Organizations die Option Delegieren aus und fügen Sie die Ressourcenrichtlinie in den Delegierungsrichtlinien-Editor ein. Wählen Sie Richtlinie erstellen aus. Öffnen Sie den Tab, auf dem Sie sich in der Security Hub Hub-Konsole befinden.
7. Wählen Sie Konfigurieren aus.

Schritt 2. Security Hub im delegierten Administratorkonto aktivieren

Das delegierte Administratorkonto schließt diesen Schritt ab. Nachdem das AWS Organisationsverwaltungskonto einen delegierten Administrator für seine Organisation bestimmt hat, muss der delegierte Administrator Security Hub für sein eigenes Konto aktivieren, bevor er die Aktivierung für die gesamte Organisation durchführen kann. AWS

So aktivieren Sie Security Hub im delegierten Administratorkonto

1. Melden Sie sich mit Ihren delegierten Administratoranmeldedaten bei Ihrem AWS Konto an. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie auf der Security Hub Hub-Startseite die Option Erste Schritte aus.
3. Im Abschnitt Sicherheitsfunktionen werden die Funktionen beschrieben, die automatisch aktiviert werden und im Basispreis pro Ressource von Security Hub enthalten sind.
4. (Optional) Legen Sie für Tags fest, ob Sie der Kontoeinrichtung ein Schlüssel-Wert-Paar hinzufügen möchten.
5. Wählen Sie Enable Security Hub, um die Aktivierung von Security Hub abzuschließen.
6. (Empfohlen) wählen Sie im Popup-Fenster Configure My Organization aus und fahren Sie mit Schritt 3 fort.

Schritt 3. Erstellen Sie eine Richtlinie, die Security Hub in allen Mitgliedskonten aktiviert

Nachdem Sie Security Hub im delegierten Administratorkonto für eine Organisation aktiviert haben, müssen Sie eine Richtlinie erstellen, die definiert, welche Dienste und Funktionen in den Mitgliedskonten der Organisation aktiviert sind. Weitere Informationen finden Sie unter Konfiguration mit einem bestimmten Richtlinientyp aktivieren.

Nachdem Sie Security Hub aktiviert haben, werden die folgenden Ressourcen in Ihrem Konto erstellt:

- Eine serviceverknüpfte Rolle namens AWSServiceRoleForSecurityHubV2.
- Service-linked Konfigurationsrekorder. Weitere Informationen finden Sie unter Service-linked Recorder in der Dokumentation zu den Security Hub Hub-Konzepten.
- Ein mit Diensten verbundener Analysator. Weitere Informationen finden Sie unter Service-linked Analyzer in der Dokumentation zu den Security Hub Hub-Konzepten.

Security Hub in einem eigenständigen Konto aktivieren

Dieses Verfahren beschreibt, wie Security Hub in einem eigenständigen Konto aktiviert wird. Ein eigenständiges Konto ist ein Konto AWS-Konto , für das keine AWS Organisationen aktiviert wurden.

So aktivieren Sie Security Hub in einem eigenständigen Konto

1. Melden Sie sich mit Ihren AWS Kontodaten bei Ihrem Konto an. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie auf der Security Hub Hub-Startseite die Option Erste Schritte aus.
3. Führen Sie im Abschnitt Sicherheitsfunktionen einen der folgenden Schritte aus:
    a. (Option 1) Wählen Sie Alle Funktionen aktivieren. Dadurch werden alle wichtigen Funktionen, Bedrohungsanalysen und zusätzliche Funktionen des Security Hub aktiviert.
    b. (Option 2) Wählen Sie Funktionen anpassen. Wählen Sie in den Abschnitten Sicherheitsmanagement, Bedrohungsanalyse und Schwachstellenmanagement die Funktionen aus, die aktiviert werden sollen. Sie können keine Funktionen abwählen, die Teil der Funktionen des Security Hub Hub-Grundplans sind.
4. Wählen Sie im Abschnitt Regionen die Option Alle Regionen aktivieren oder Bestimmte Regionen aktivieren aus. Wenn Sie „Alle Regionen aktivieren“ wählen, können Sie festlegen, ob

neue Regionen automatisch aktiviert werden sollen. Wenn Sie Bestimmte Regionen aktivieren wählen, müssen Sie auswählen, welche Regionen Sie aktivieren möchten.

5. (Optional) Fügen Sie für Ressourcen-Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Konfiguration leichter identifizieren können.
6. Wählen Sie Enable Security Hub (Security Hub aktivieren).

Nachdem Sie Security Hub aktiviert haben, werden die folgenden Ressourcen in jedem Konto erstellt, in dem Sie den Dienst aktiviert haben:

- Eine mit dem Dienst verknüpfte Rolle namens AWSServiceRoleForSecurityHubV2.
- Service-linked Konfigurationsrekorder. Weitere Informationen finden Sie unter Service-linked Recorder in der Dokumentation zu den Security Hub Hub-Konzepten.
- Ein mit Diensten verbundener Analysator. Weitere Informationen finden Sie unter Service-linked Analyzer in der Dokumentation zu den Security Hub Hub-Konzepten.

Benennung eines delegierten Administrators in Security Hub

Im Verwaltungskonto der AWS Organisation können Sie einen delegierten Administrator für Ihre Organisation benennen. Es hat sich bewährt, für alle Sicherheitsdienste denselben delegierten Administrator zu verwenden, um eine einheitliche Verwaltung zu gewährleisten.

Das Verfahren in diesem Thema beschreibt, wie Sie einen delegierten Administrator in Security Hub benennen. Es wird davon ausgegangen, dass Sie Security Hub zuvor aktiviert haben, aber während des Aktivierungs-Workflows keinen delegierten Administrator benannt haben.

Überlegungen

Beachten Sie bei der Benennung eines delegierten Administrators in Security Hub Folgendes:

- Das Verwaltungskonto der AWS Organisation kann sich selbst als delegierter Administrator in Security Hub CSPM benennen, aber nicht selbst als delegierter Administrator in Security Hub. In diesem Szenario muss das Verwaltungskonto einen anderen zum delegierten Administrator in Security Hub AWS-Konto benennen.
- Wenn das Verwaltungskonto der AWS Organisation einen delegierten Administrator in Security Hub CSPM benennt, wird dieser delegierte Administrator automatisch zum delegierten Administrator in Security Hub. In diesem Szenario erlaubt Security Hub nur dieser Person, als delegierter Administrator zu fungieren. AWS-Konto

> **Note**
>
> Wenn der delegierte Administrator entweder über die Security Hub CSPM-Konsole, die Security Hub-Konsole oder die AWS Organizations API entfernt wird, wird er aus beiden Diensten entfernt. Wenn der delegierte Administrator aus Security Hub CSPM entfernt wird, wird die zentrale Konfiguration automatisch deaktiviert.

Benennung eines delegierten Administrators nach der Aktivierung von Security Hub

Dieses Verfahren muss vom Verwaltungskonto der AWS Organisation abgeschlossen werden. Es wird davon ausgegangen, dass das Verwaltungskonto der AWS Organisation zuvor Security Hub aktiviert hat, während des Aktivierungs-Workflows jedoch kein delegierter Administrator benannt wurde.

> **Note**
>
> Nachdem Sie dieses Verfahren abgeschlossen haben, müssen Sie eine Richtlinie erstellen, die es dem delegierten Administrator Ihrer Organisation ermöglicht, Security Hub zu konfigurieren und bestimmte Aktionen darin durchzuführen. AWS Organizations Weitere Informationen finden Sie unter Erstellen der Richtlinie für delegierte Administratoren in Security Hub.

So benennen Sie einen delegierten Administrator in Security Hub

1. Melden Sie sich mit den Anmeldeinformationen Ihres Organisationsverwaltungskontos bei Ihrem Konto an und öffnen Sie die Security Hub-Konsole unter. AWS https://console.aws.amazon.com/securityhub/v2/home
2. Wählen Sie im Navigationsbereich Allgemein aus.
3. Wählen Sie unter Delegierter Administrator die Option Konfigurieren aus. Wählen Sie eine der bereitgestellten Optionen aus AWS-Konten, oder geben Sie die 12-stellige AWS-Konto Nummer für den ein AWS-Konto , den Sie als delegierten Administrator für Ihre Organisation benennen möchten. Wählen Sie Speichern.

Erstellen der delegierten Administratorrichtlinie in Security Hub

Das Verwaltungskonto der AWS Organisation kann eine Richtlinie erstellen, die es dem delegierten Administrator ermöglicht, Security Hub zu konfigurieren und darin bestimmte Aktionen durchzuführen. AWS Organizations Das Verfahren in diesem Thema beschreibt, wie die Richtlinie erstellt wird. Wenn Sie das Verfahren abgeschlossen haben, können Sie Security Hub erlauben, die Richtlinie für Sie zu erstellen, oder Sie können die Richtlinie manuell erstellen. Erlauben Sie Security Hub, die Richtlinie zu erstellen, sofern Sie sie nicht für einen bestimmten Anwendungsfall anpassen möchten.

Führen Sie dieses Verfahren nur durch, wenn das Verwaltungskonto der Organisation Security Hub aktiviert und einen delegierten Administrator benannt hat, aber die Erstellung der Richtlinie während des Aktivierungs-Workflows übersprungen wurde. Informationen zur Aktualisierung dieser Richtlinie finden Sie im Benutzerhandbuch unter Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie. AWS Organizations AWS Organizations

> **Note**
>
> Nachdem Sie dieses Verfahren abgeschlossen haben, kann der delegierte Administrator eine Richtlinie zur Verwaltung von Mitgliedskonten in Ihrer Organisation erstellen. Weitere Informationen finden Sie unter Erstellen einer Richtlinie als delegierter Administrator zur Verwaltung von Mitgliedskonten.

So erstellen Sie die Richtlinie für delegierte Administratoren

1. Melden Sie sich mit den Anmeldedaten Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Allgemein aus.
3. Führen Sie für die Richtlinie für delegierte Administratoren einen der folgenden Schritte aus:
   - Wählen Sie Richtlinie erstellen aus. Wählen Sie das Kästchen unter der Richtlinienerklärung aus, um zu bestätigen, dass Security Hub automatisch eine Delegierungsrichtlinie erstellt, die dem delegierten Administrator alle erforderlichen Berechtigungen gewährt.
   - Öffnen Sie die Richtlinie. Wählen Sie Kopieren und anhängen. Wählen Sie in der AWS Organizations Konsole unter Delegierter Administrator für die Option Delegieren aus AWS Organizations, und fügen Sie die Ressourcenrichtlinie in den Editor für Delegationsrichtlinien

ein. Wählen Sie Richtlinie erstellen aus. Öffnen Sie in der Security Hub-Konsole die Registerkarte, auf der Sie sich befinden, und wählen Sie Konfigurieren aus.

Verwaltung der Konfiguration von Mitgliedskonten in einem AWS Organisation

Der delegierte Administrator einer AWS Organisation kann Sicherheitsfunktionen für Mitgliedskonten und Regionen konfigurieren. Zwei Arten von Konfigurationen sind verfügbar: Richtlinien und Bereitstellungen. Richtlinien generieren AWS Unternehmensrichtlinien für Konten und Regionen für AWS Security Hub und Amazon Inspector. Bereitstellungen sind eine einmalige Aktion, um eine Sicherheitsfunktion für ausgewählte Konten und Regionen für Amazon GuardDuty und AWS Security Hub CSPM zu aktivieren. Im Gegensatz zu Richtlinien können Sie Bereitstellungen nicht anzeigen oder bearbeiten, und Bereitstellungen gelten nicht für neu aktivierte Konten. Als Alternative sind Funktionen zur automatischen Aktivierung für neue Mitgliedskonten in Amazon GuardDuty und AWS Security Hub CSPM verfügbar.

Security Hub-Konfigurationskatalog

Der Konfigurationskatalog von Security Hub bietet mehrere Optionen, mit denen Sie Ihre AWS Unternehmenskonten für die von Security Hub bereitgestellten Sicherheitsfunktionen konfigurieren können.

Die folgenden Optionen sind im Security Hub-Konfigurationskatalog verfügbar.

Security Hub (wichtige und zusätzliche Funktionen)

Dies ist die empfohlene Konfiguration für die Bereitstellung für Security Hub.

Typ: Richtlinie und Bereitstellungen

Beschreibung: Diese Konfiguration aktiviert die grundlegenden Funktionen für Sicherheitsmanagement, Statusmanagement, Bedrohungsanalyse und Schwachstellenmanagement von Security Hub. Sie ermöglicht optional zusätzliche Funktionen.

Bedrohungsanalysen von GuardDuty

Typ: Einsatz

Beschreibung: Aktivieren Sie ausgewählte GuardDuty Amazon-Funktionen, um AWS Datenquellen und Protokolle in Ihrer AWS Umgebung kontinuierlich zu überwachen, zu analysieren und zu verarbeiten.

Haltungsmanagement von AWS Security Hub CSPM

Typ: Bereitstellung

Beschreibung: Diese Konfiguration aktiviert die Standards und Kontrollen von Security Hub CSPM, die erkennen, wenn Ihre AWS Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Schwachstellenmanagement von Amazon Inspector

Typ: Richtlinie

Beschreibung: Diese Konfiguration aktiviert ausgewählte Amazon Inspector-Funktionen, die Workloads, Instances, Container-Images und andere Ressourcen automatisch erkennen und sie nach Sicherheitslücken und Netzwerkrisiken durchsuchen.

Aktivierung einer Konfiguration mit einem Richtlinientyp

Das folgende Verfahren beschreibt, wie Sie eine Konfiguration mit einem Richtlinientyp für Ihre AWS Organisationskonten erstellen. Um eine Konfigurationsrichtlinie zu erstellen, müssen Sie zunächst die Richtlinie für delegierte Administratoren im Verwaltungskonto der AWS Organisation erstellen. Informationen zum Erstellen der Richtlinie für delegierte Administratoren in Security Hub finden Sie unter Erstellen der Richtlinie für delegierte Administratoren in Security Hub.

So erstellen Sie eine Richtlinie, die Mitgliedskonten aktiviert und deaktiviert

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.
3. Wählen Sie im Konfigurationskatalog ein Element mit einem Richtlinientyp oder einer Richtlinie und Bereitstellung aus. Um Security Hub vollständig zu konfigurieren, wählen Sie Security Hub (grundlegende und zusätzliche Funktionen).
4. Geben Sie auf der Seite Security Hub konfigurieren im Abschnitt Details einen Namen und eine Beschreibung für die Richtlinie ein.

5. Wählen Sie im Abschnitt Sicherheitsfunktionen eine der folgenden Optionen aus:

   - Alle Funktionen aktivieren — Aktiviert alle wichtigen Funktionen, Bedrohungsanalysen und zusätzlichen Funktionen von Security Hub.
   - Funktionen anpassen — Wählen Sie Funktionen aus den Abschnitten Sicherheitsmanagement, Bedrohungsanalyse und Schwachstellenmanagement aus. Sie können Funktionen, die Teil des Security Hub Essential-Plans sind, nicht abwählen.

6. Wählen Sie im Abschnitt Kontoauswahl eine der folgenden Optionen:

   - Alle Organisationseinheiten und Konten — Wendet die Konfiguration auf Ihre gesamte Organisation an.
   - Bestimmte Organisationseinheiten und Konten — Verwenden Sie die Suchleiste oder den Organisationsstrukturbaum, um die Organisationseinheiten und Konten auszuwählen, für die die Richtlinie gilt.
   - Keine Organisationseinheiten oder Konten — Wendet die Konfiguration nicht auf Organisationseinheiten oder Konten an.

7. Wählen Sie im Abschnitt Regionen eine der folgenden Optionen aus:

   - Alle Regionen aktivieren — Wählen Sie optional aus, ob neue Regionen automatisch aktiviert werden sollen.
   - Alle Regionen deaktivieren — Wählen Sie optional aus, ob neue Regionen automatisch deaktiviert werden sollen.
   - Regionen angeben — Wählen Sie aus, welche Regionen aktiviert und deaktiviert werden sollen.

8. (Optional) Erweiterte Einstellungen finden Sie im AWS Organizations Benutzerhandbuch unter Vererbungsoperatoren.
9. (Optional) Fügen Sie für Ressourcen-Tags Tags als Schlüssel-Wert-Paare hinzu, um die Konfiguration leichter identifizieren zu können.
10. Wählen Sie Weiter aus.
11. Überprüfen Sie Ihre Änderungen und wählen Sie dann Anwenden.

    Der Konfigurationsstatus Ihrer Richtlinie wird oben auf der Seite „Richtlinien“ angezeigt. Jede Funktion bietet einen Status, der angibt, ob sie erfolgreich konfiguriert wurde oder ob bei der Bereitstellung Fehler aufgetreten sind. Bei etwaigen Fehlern klicken Sie auf den Link „Fehler“, um weitere Informationen zu erhalten. Die geltenden Richtlinien auf Kontoebene finden Sie auf der Seite „Konfigurationen“ auf der Registerkarte „Organisation“.

Aktivierung einer Konfiguration mit einem Bereitstellungstyp

Das folgende Verfahren beschreibt, wie Sie eine Konfiguration mit einem Bereitstellungstyp für Ihre AWS Organisationskonten erstellen.

So erstellen Sie eine Bereitstellung, die Mitgliedskonten aktiviert

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.
3. Wählen Sie ein Element mit einem Bereitstellungstyp aus dem Konfigurationskatalog aus.
4. Wählen Sie im Abschnitt Sicherheitsfunktionen die Sicherheitsfunktionen aus, die Sie aktivieren möchten.
5. Wählen Sie im Abschnitt Kontoauswahl eine der folgenden Optionen aus:
   - Alle Organisationseinheiten und Konten — Wendet die Bereitstellung auf Ihre gesamte Organisation an.
   - Bestimmte Organisationseinheiten und Konten — Verwenden Sie die Suchleiste oder den Organisationsstrukturbaum, um die Organisationseinheiten und Konten auszuwählen, für die die Bereitstellung gilt.
   - Keine Organisationseinheiten oder Konten — Wendet die Bereitstellung nicht auf eine Organisationseinheit oder ein Konto an.
6. Wählen Sie im Abschnitt Regionen eine der folgenden Optionen aus:
   - Alle Regionen aktivieren — Wählen Sie optional aus, ob neue Regionen automatisch aktiviert werden sollen.
   - Alle Regionen deaktivieren — Wählen Sie optional aus, ob neue Regionen automatisch deaktiviert werden sollen.
   - Regionen angeben — Wählen Sie aus, welche Regionen aktiviert und deaktiviert werden sollen.
7. Wählen Sie Konfigurieren aus.

Eine Konfigurationsrichtlinie bearbeiten

Sie können die Funktionen, Regionen und Konten bearbeiten, die einer Konfigurationsrichtlinie zugeordnet sind. Wenn Sie eine Richtlinie zur Bearbeitung öffnen, zeigt die Konsole die aktuelle Konfiguration an.

> **Note**
>
> Änderungen gelten nur für die Funktionen, die Sie in der aktualisierten Richtlinie auswählen. Nicht ausgewählte Funktionen behalten ihre bestehende Konfiguration für die Konten und Regionen in der Richtlinie bei.

Um eine Konfigurationsrichtlinie zu bearbeiten

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.
3. Wählen Sie auf der Registerkarte Konfigurierte Richtlinien das Optionsfeld für die Richtlinie aus, die Sie bearbeiten möchten, und wählen Sie dann Bearbeiten aus.
4. Wählen Sie im Abschnitt „Fähigkeit“ eine der folgenden Optionen aus:
   - Alle Funktionen konfigurieren und aktivieren — Aktiviert alle Funktionen in der Richtlinie.
   - Wählen Sie einzelne Funktionen aus und wählen Sie für jede einzelne Funktion die Option Aktivieren , Deaktivieren oder Benutzerdefiniert.
5. Wählen Sie im Abschnitt Kontoauswahl eine der folgenden Optionen aus:
   - Alle Organisationseinheiten und Konten — Wendet die Richtlinie auf Ihre gesamte Organisation an.
   - Bestimmte Organisationseinheiten und Konten — Verwenden Sie die Suchleiste oder den Organisationsstrukturbaum, um die Organisationseinheiten und Konten auszuwählen, für die die Richtlinie gilt.
   - Keine Organisationseinheiten oder Konten — Entfernt die Richtlinie aus allen Zielen.
6. Konfigurieren Sie im Abschnitt Regionen, für welche Regionen die Richtlinie gilt. Die Optionen hängen von Ihrer Auswahl an Fähigkeiten ab.

Wenn Sie sich dafür entschieden haben, alle Funktionen zu aktivieren:

- Für alle ausgewählten Funktionen — Legt dieselbe Regionskonfiguration für alle Funktionen fest.
- Pro Fähigkeit — Ermöglicht es Ihnen, Regionen für jede Funktion einzeln auszuwählen.

Wählen Sie dann Alle Regionen aktivieren (mit der Option, automatisch neue Regionen zu aktivieren) oder In einigen Regionen aktivieren, um bestimmte Regionen auszuwählen.

Wenn du gemischte Aktionen (aktivieren, deaktivieren oder benutzerdefiniert) für einzelne Funktionen ausgewählt hast:

- Wenn alle ausgewählten Funktionen dieselbe Aktion verwenden, wählen Sie Alle ausgewählten Funktionen aus, um die Regionen einheitlich festzulegen. Um Regionen für jede Fähigkeit einzeln festzulegen, wählen Sie Pro Fähigkeit aus.
- Wenn Funktionen unterschiedliche Aktionen haben, müssen Sie Regionen für jede Fähigkeit einzeln zuweisen.
- Wählen Sie für Funktionen mit der Aktion „Benutzerdefiniert“ die Option Für alle ausgewählten Funktionen aus, um Regionen für alle Funktionen einheitlich festzulegen. Um Regionen für jede Funktion separat zu konfigurieren, wählen Sie Pro Fähigkeit aus.

7. Wählen Sie Weiter aus.
8. Überprüfen Sie die Änderungen und klicken Sie dann auf Update (Aktualisieren). Die aktualisierte Richtlinie konfiguriert die Zielkonten.

Löschen einer Konfigurationsrichtlinie

Sie können eine Konfigurationsrichtlinie löschen. Wenn Sie eine Richtlinie löschen, entfernt der Dienst alle angehängten Konten und Organisationseinheiten aus der Richtlinie.

So löschen Sie eine Konfigurationsrichtlinie

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.

3. Wählen Sie auf der Registerkarte Konfigurierte Richtlinien die Richtlinie aus, die Sie löschen möchten, und klicken Sie dann auf Löschen.
4. Geben Sie `delete` in das Bestätigungsfeld ein, und wählen Sie dann Löschen aus.

Entfernen des delegierten Administratorkontos in Security Hub

Sie können das delegierte Administratorkonto jederzeit in der Security Hub-Konsole entfernen. Durch diese Aktion wird der delegierte Administrator jedoch sowohl aus Security Hub als auch aus Security Hub CSPM entfernt. Wir empfehlen, diese Aktion nur durchzuführen, wenn Sie diesen Vorgang mit Ihrem Sicherheitskonto bestätigt haben.

> **Note**
>
> Wenn Sie als delegierter Security Hub CSPM-Administrator ein anderes Konto als das Verwaltungskonto der Organisation verwenden, wird es auch aus Security Hub entfernt, wenn Sie es entweder über die Security Hub CSPM-Konsole oder die AWS Organizations API entfernen.
> Wenn Sie den delegierten Security Hub-Administrator entweder über die Security Hub-Konsole oder die AWS Organizations API entfernen, wird er ebenfalls aus Security Hub CSPM entfernt. Wenn der delegierte Administrator aus Security Hub CSPM entfernt wird, wird die zentrale Konfiguration automatisch deaktiviert.

Um das Konto des delegierten Administrators zu entfernen

1. Melden Sie sich mit den Anmeldedaten Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Allgemein aus.
3. Wählen Sie unter Delegierter Administrator die Option Delegierten Administrator entfernen aus. Geben Sie im Bestätigungsdialogfeld entfernen ein und wählen Sie Entfernen aus.

Re-enabling Sicherheits-Hub

Bevor Sie Security Hub für Konten erneut aktivieren, die zuvor mithilfe einer Security Hub-Richtlinie deaktiviert wurden, müssen Sie zunächst die Deaktivierungsrichtlinie trennen. Wenn Sie versuchen,

Security Hub erneut zu aktivieren, während dem Konto oder der Organisationseinheit noch eine Deaktivierungsrichtlinie zugeordnet ist, überschreibt die Deaktivierungsrichtlinie die Aktivierung und Security Hub bleibt deaktiviert.

So entfernen Sie die Security Hub-Deaktivierungsrichtlinie für eine Organisation oder ein Konto

1. Melden Sie sich mit Ihrem AWS Konto mit den Anmeldedaten für das Verwaltungskonto Ihrer Organisation an. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/v2/home.
2. Wählen Sie im Navigationsbereich AWS Konten aus.
3. Wenn die aktuelle Security Hub-Deaktivierungsrichtlinie für Ihre gesamte Organisation galt, wählen Sie Root unter der Organisationsstruktur aus. Wenn die aktuelle Security Hub-Deaktivierungsrichtlinie für bestimmte Konten gilt, wählen Sie das entsprechende Konto in der Organisationsstruktur aus und folgen Sie dann den verbleibenden Schritten für jedes Konto.
4. Suchen Sie auf der Registerkarte Richtlinien den Abschnitt mit dem Titel Security Hub-Richtlinien.
5. Wählen Sie das Optionsfeld neben der Richtlinie, die Security Hub deaktiviert. Wählen Sie Trennen aus.

Nachdem Sie die Richtlinie von Ihrer Organisation oder Ihren Konten getrennt haben, können Sie Security Hub wieder aktivieren. Weitere Informationen zur erneuten Aktivierung von Security Hub finden Sie unter Konfiguration von Mitgliedskonten in einer AWS Organisation verwalten.

Security Hub Hub-Empfehlungen

Die folgenden Sicherheitsdienste AWS senden Ergebnisse im OCSF-Format an Security Hub. Nachdem Sie Security Hub aktiviert haben, aktivieren Sie diese AWS-Services für zusätzliche Sicherheit.

Security Hub CSPM

Wenn Sie Security Hub CSPM aktivieren, erhalten Sie einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Auf diese Weise können Sie Ihre Umgebung anhand von Industriestandards und bewährten Methoden beurteilen. Sie können zwar mit Security Hub beginnen, ohne Security Hub CSPM zu aktivieren, aber die Aktivierung von Security Hub CSPM ermöglicht es Security Hub, Sicherheitssignale von Security Hub CSPM zu korrelieren, um Ihr Statusmanagement zu verbessern.

Wenn Sie Security Hub CSPM aktivieren, empfehlen wir außerdem, den Standard AWS Foundational Security Best Practices für Ihr Konto zu aktivieren. Dieser Standard besteht aus einer Reihe von Kontrollen, die erkennen, wenn Sie AWS-Konten und Ihre Ressourcen von den bewährten Sicherheitsmethoden abweichen. Wenn Sie den Standard AWS Foundational Security Best Practices für Ihr Konto aktivieren, aktiviert AWS Security Hub CSPM automatisch alle seine Kontrollen, einschließlich der Kontrollen für die folgenden Ressourcentypen:

- Kontokontrollen
- Amazon DynamoDB-Steuerelemente
- Amazon Elastic Compute Cloud-Steuerelemente
- AWS Identity and Access Management (IAM) -Steuerelemente
- AWS Lambda Steuerungen
- Steuerelemente für Amazon Relational Database Service (Amazon RDS)
- Steuerelemente von Amazon Simple Storage Service

Sie können alle Steuerelemente in dieser Liste deaktivieren. Wenn Sie jedoch eines dieser Steuerelemente deaktivieren, können Sie keine Expositionsergebnisse für unterstützte Ressourcen erhalten. Informationen zu Kontrollen, die für den Standard AWS Foundational Security Best Practices gelten, finden Sie unter AWS Foundational Security Best Practices v1.0.0 (FSBP).

GuardDuty

Wenn Sie die GuardDuty Option aktivieren, können Sie alle Ihre Ergebnisse zu Bedrohungen und Sicherheitsvorkehrungen im Dashboard der Security Hub Hub-Konsole einsehen. Wenn Sie diese Option aktivieren GuardDuty, GuardDuty wird automatisch mit dem Senden von Daten an Security Hub im OCSF-Format begonnen.

Amazon Inspector

Wenn Sie Amazon Inspector aktivieren, können Sie alle Ihre Risiken und Ergebnisse zur Sicherheitsabdeckung im Dashboard der Security Hub Hub-Konsole einsehen. Wenn Sie Amazon Inspector aktivieren, beginnt Amazon Inspector automatisch, Daten im OCSF-Format an Security Hub zu senden.

Wir empfehlen, das Amazon EC2-Scannen und das Lambda-Standardscannen zu aktivieren. Wenn Sie Amazon EC2-Scanning aktivieren, scannt Amazon Inspector Amazon EC2 EC2-Instances in Ihrem Konto auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Wenn Sie das Lambda-Standardscannen aktivieren, scannt Amazon Inspector Lambda-Funktionen auf

Softwareschwachstellen in Paketabhängigkeiten. Weitere Informationen finden Sie unter Aktivierung eines Scan-Typs im Amazon Inspector Inspector-Benutzerhandbuch.

Macie

Wenn Sie Macie aktivieren, können Sie zusätzliche Risiken für Ihre Amazon S3 S3-Buckets erkennen. Wir empfehlen, die automatische Erkennung sensibler Daten zu konfigurieren, damit Macie Ihr Amazon S3 S3-Bucket-Inventar täglich auswerten kann.

Kontoabdeckung im Security Hub

Auf der Seite Kontoabdeckung wird angezeigt, für welche Konten und Regionen in Ihrer Organisation Security Hub und die integrierten Sicherheitsfunktionen aktiviert sind. Zu diesen Funktionen gehören Dienste wie Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM und Amazon Macie. Verwenden Sie diese Seite, um Deckungslücken zu identifizieren und die Einführung von Funktionen in Ihrem Unternehmen zu verfolgen.

Seite zur Kontoabdeckung

Auf der Seite zur Kontoabdeckung können Sie sich aggregierte Kennzahlen zum Versicherungsschutz ansehen. Auf der Registerkarte Konten finden Sie Details auf Kontoebene und auf der Registerkarte Ergebnisse zur Deckung können Sie spezifische Deckungslücken überprüfen.

So greifen Sie auf den Security Hub zu Kontoabdeckung angezeigten

1. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoabdeckung aus.

Abschnitt „Übersicht“

Im Bereich Übersicht werden aggregierte Kennzahlen zum Sicherheitsschutz für alle überwachten Konten angezeigt. Für delegierte Administratorkonten werden in diesem Abschnitt Details zur Aktivierung von Security Hub im gesamten Unternehmen angezeigt, sodass Sie einen Überblick über den Schutz aller Mitgliedskonten erhalten. Diese übergeordnete Visualisierung zeigt den Prozentsatz der Konten mit Security Hub und allen aktivierten Sicherheitsfunktionen und bietet so einen umfassenden Überblick über Ihren Sicherheitsstatus. Sie können den Prozentsatz der Security Hub Hub-Abdeckung auswählen, um eine Aufschlüsselung der aktivierten Konten nach Regionen

anzuzeigen. Sie können die einzelnen Funktionen in Prozent auswählen, um die Ergebnisse der Abdeckung nach dieser Funktion zu filtern.

Die Prozentsätze im Abschnitt „Übersicht“ werden anhand der folgenden Berechnungen ermittelt:

- Security Hub-Aktivierung = (Anzahl der Konto- und Regionspaare, in denen Security Hub aktiviert ist) ÷ (Gesamtzahl der Konten in Ihrer Organisation × Regionen, in denen Security Hub verfügbar ist)
- Serviceabdeckung = (Anzahl der aktivierten Konto- und konfigurierten Regionspaare, in denen die Funktion aktiviert ist) ÷ (Gesamtzahl der aktivierten Konto- und konfigurierten Regionspaare in konfigurierten Regionen, in denen das Konto aktiviert ist und die Funktion verfügbar ist)

> **Konfigurierte Regionen**
>
> Bei der Einrichtung einer Heimatregion umfassen die konfigurierten Regionen die Heimatregion und verknüpfte Regionen. Bei allen anderen Setups beziehen sich die konfigurierten Regionen nur auf die aktuelle Region.

Registerkarte „Konten“

Diese Registerkarte ist nur im delegierten Security Hub-Administratorkonto verfügbar. Verwenden Sie den Tab Konten, um den kontospezifischen Versicherungsschutz zu analysieren. In der Spalte Security Hub wird die Anzahl der Regionen angezeigt, in denen Security Hub für jedes Konto aktiviert ist. Diese Spalte wird nicht angezeigt, wenn der Tab in Opt-in-Regionen (Regionen, die standardmäßig deaktiviert sind) aufgerufen wird. Für jede Sicherheitsfunktion wird ein Prozentsatz der Abdeckung angezeigt. Wenn diese Option ausgewählt ist, wird eine detaillierte Aufschlüsselung der einzelnen Funktionen und ihres prozentualen Schutzes innerhalb dieser Funktion angezeigt. Wenn Sie diese Prozentsätze auswählen, filtert Security Hub die Ergebnisse, um die Abdeckung für diese Funktion und dieses Konto anzuzeigen.

Die Prozentsätze auf der Registerkarte Konten werden anhand der folgenden Berechnung ermittelt:

Geltungsbereich der Registerkarte „Konten“ = (Anzahl der Regionen, in denen die Funktion aktiviert ist) — (Regionen, in denen die Funktion verfügbar ist)

Es gibt mehrere Fälle, in denen der Prozentsatz der Abdeckung als 0% angezeigt werden kann:

- Security Hub ist im Konto nicht aktiviert, sodass keine Deckungsergebnisse erfasst werden.

- Security Hub wartet darauf, dass die Ergebnisse zur Berichterstattung generiert werden.

Registerkarte „Ergebnisse des Versicherungsschutzes“

Auf der Registerkarte „Ergebnisse zum Versicherungsschutz“ finden Sie Informationen zu Sicherheitsfunktionen, die in Ihren Konten und Regionen aktiviert oder deaktiviert sind. Diese Ergebnisse helfen dabei, Bereiche zu identifizieren, in denen der Sicherheitsschutz verbessert werden kann. Für jedes Ergebnis werden der Titel des Ergebnisses, das betroffene Konto und die betroffene Region sowie der aktuelle Status angezeigt. Zu jedem Ergebnis gehört auch ein Link zur Konfiguration, über den Sie zu dem jeweiligen Dienst gelangen, über den Sie die Konfiguration für diese Funktion verwalten können, oder zur Security Hub Hub-Konfigurationsseite, auf der Sie Ihre Konfigurationen für Sicherheitsdienste aktualisieren können.

Sie können Deckungsergebnisse mit dem Status Nicht abgedeckt unterdrücken, wenn diese Sicherheitsfunktion nicht für die Kombination aus Konto und Region gilt. Security Hub schließt unterdrückte Ergebnisse bei der Berechnung des Prozentsatzes der Sicherheitsabdeckung aus.

Weitere Informationen zu Deckungsergebnissen und deren Unterdrückung finden Sie unter Deckungsergebnisse in Security Hub.

Widget „Sicherheitsabdeckung“

Die Kontoabdeckung kann auch über das Widget Sicherheitsabdeckung im Security Hub Hub-Übersichts-Dashboard angezeigt werden. Weitere Informationen finden Sie unter Widget „Sicherheitsabdeckung“.

Erweiterter Tarif für Security Hub

Mit dem Security Hub Extended-Plan können Sie Ihren gesamten Unternehmensumfang in Bezug auf Cloud, Endpunkt, Netzwerk, Identität, Daten, E-Mail und Browser schützen. Nutzen Sie AWS Security Hub als Mittelpunkt eines integrierten Sicherheitserlebnisses. Mit dem Security Hub Extended-Plan können Sie Partnerlösungen auswählen, die Ihren Sicherheitsanforderungen entsprechen, und sich für flexible Pay-as-you-go-Preise anmelden, ohne dass Vorabinvestitionen oder langfristige Verpflichtungen erforderlich sind. Sie können Partnerlösungen hinzufügen oder entfernen, wenn sich Ihre Geschäftsanforderungen ändern.

Der Security Hub Extended-Plan steht allen Kunden zur Verfügung, die den Security Hub Essentials-Plan aktiviert haben. Die Gebühren für den Security Hub Extended-Tarif erscheinen auf Ihrer monatlichen AWS Rechnung, wenn Sie AWS als Verkäufer eingetragen sind.

Die Preise für den Security Hub-Erweiterungsplan für alle Lösungen finden Sie auf der Seite mit den Security Hub-Preisdetails auf der Registerkarte Erweiterter Tarif.

Berechtigungen für den Security Hub Extended-Tarif

Um ein Partnerprodukt aus dem Security Hub Extended-Plan zu abonnieren, benötigen Sie zusätzlich zu Ihren Security Hub-Berechtigungen die folgenden Berechtigungen:

- `aws-marketplace:ViewSubscriptions`
- `aws-marketplace:Subscribe`

Um ein Partnerprodukt im Security Hub Extended-Tarif abzubestellen, benötigen Sie zusätzlich zu Ihren Security Hub-Berechtigungen die folgenden Berechtigungen:

- `license-manager:ListReceivedLicenses`
- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

Weitere Informationen zu AWS Marketplace-Berechtigungen finden Sie unter Steuern des Zugriffs auf AWS Marketplace-Abonnements im AWS Marketplace-Käuferleitfaden.

Prüfung und Registrierung für Partner mit erweitertem Tarif

Auf den Security Hub Extended-Plan kann über das delegierte Security Hub-Administratorkonto oder über eigenständige Konten zugegriffen werden. Auf der Security Hub Extended-Abonnementseite können Sie Details zu jedem Partner einsehen, ein Abonnement für eine Partnerlösung abschließen und den Onboarding-Prozess für die Lösungen jedes Partners über die Onboarding-Seite des Partners beginnen.

Um auf den Security Hub Extended-Plan zuzugreifen und sich für das Produkt eines Partners zu registrieren

1. Melden Sie sich mit den Anmeldedaten Ihres delegierten Administrators oder eines eigenständigen Kontos an der AWS Management Console an.
2. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
3. Wählen Sie im Navigationsbereich Verwaltung und dann Erweiterter Tarif aus.

4. Wählen Sie für jede Partnerlösung, für die Sie sich registrieren möchten, die Option Produkt anzeigen aus.
5. Überprüfen Sie die Produktpreisdetails und wählen Sie dann Abonnieren, wenn Sie bereit sind, mit dem Onboarding für das Partnerprodukt zu beginnen.
6. Wählen Sie nach Abschluss des Abonnementvorgangs die Option Konto einrichten aus, um zur Anmeldeseite des Partners weitergeleitet zu werden.
7. Geben Sie die erforderlichen Informationen für die Partner-Anmeldeseite ein und folgen Sie den nächsten vom Partner bereitgestellten Schritten, um die Onboarding-Schritte abzuschließen.

> **Important**
>
> Die Partnerlösung wird Ihnen erst in Rechnung gestellt, wenn Sie den Onboarding-Prozess für das Partnerprodukt abgeschlossen haben.

Abmeldung von einem Partner mit erweitertem Tarif

Wenn Sie eine Partnerlösung mit erweitertem Tarif nicht mehr nutzen möchten, können Sie sich von der Partnerliste abmelden.

Um sich von einer Partnerlösung abzumelden, folgen Sie den Anweisungen unter Kündigen Ihres SaaS-Abonnements im AWS Marketplace Buyer Guide.

> **Important**
>
> Neben der Kündigung Ihres Abonnements sollten Sie alle zusätzlichen Offboarding-Schritte befolgen, die für die Partnerlösung erforderlich sind, je nachdem, wie Sie die Lösung für Ihr Unternehmen konfiguriert haben.

Grundlegendes zur regionsübergreifenden Aggregation in Security Hub

Wenn Sie die regionsübergreifende Aggregation in Security Hub aktivieren, legen Sie eine Heimatregion fest. Die Heimatregion sammelt Erkenntnisse, Ressourcen und Trends aus einer oder

mehreren verknüpften Regionen. Anschließend können Sie alle Sicherheitsdaten aus einer einzigen Region verwalten.

Angenommen, Sie legen USA Ost (Nord-Virginia) als Heimatregion und USA West (Oregon) und USA West (Nordkalifornien) als verknüpfte Regionen fest. Wenn Sie die Ergebnisseite in USA Ost (Nord-Virginia) aufrufen, sehen Sie die Ergebnisse aus allen drei Regionen. Aktualisierungen dieser Ergebnisse spiegeln sich auch in allen drei Regionen wider.

Arten von Daten, die aggregiert sind

Wenn die regionsübergreifende Aggregation mit einer oder mehreren verknüpften Regionen aktiviert ist, repliziert Security Hub die folgenden Daten aus den verknüpften Regionen in die Heimatregion. Dies geschieht in jedem Konto, für das die regionsübergreifende Aggregation aktiviert ist.

- Ergebnisse
- Ressourcen
- Trends
- Software- und Paketinventar (ab November 2026)

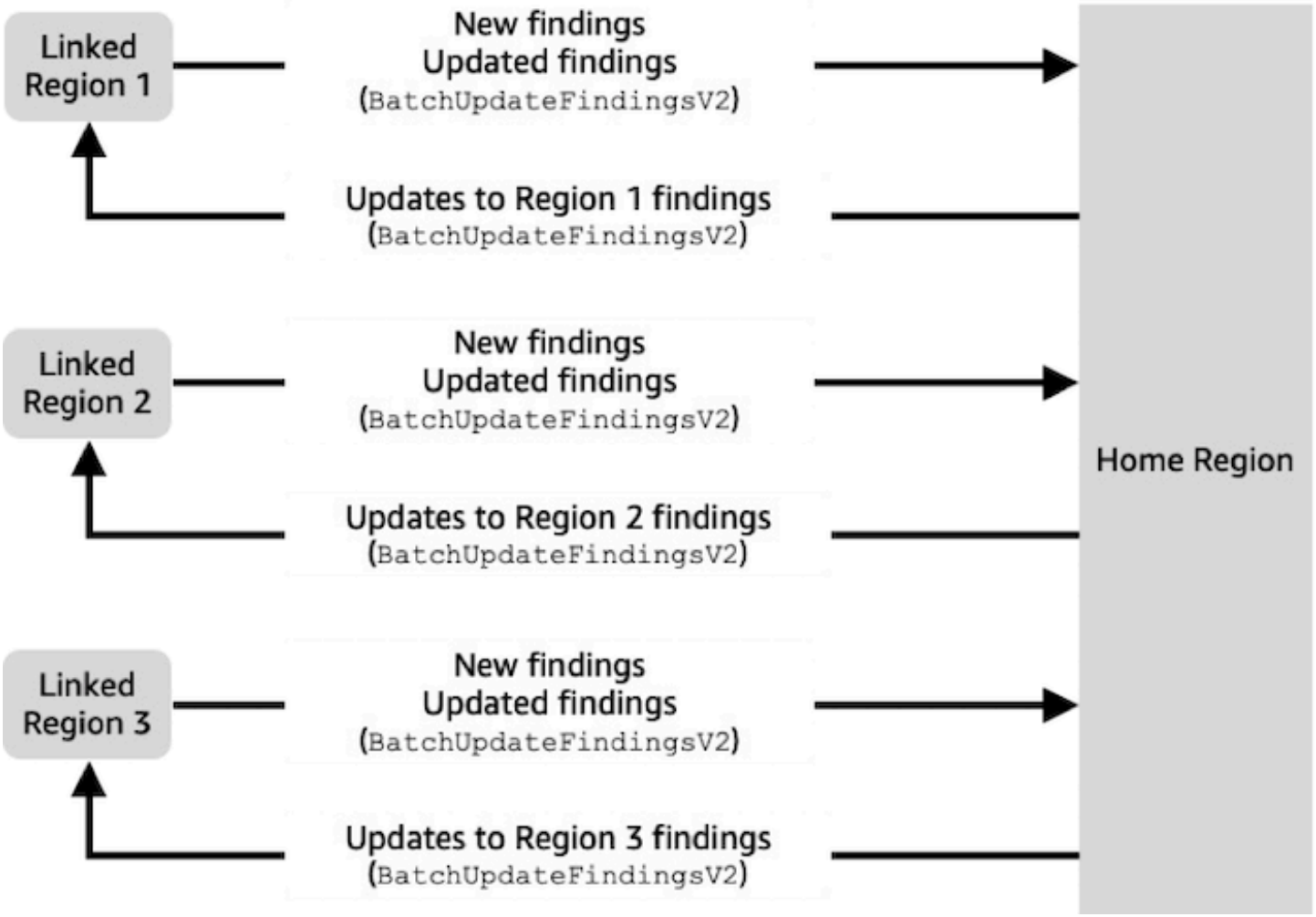
Zusätzlich zu den neuen Daten in der vorherigen Liste repliziert Security Hub auch Aktualisierungen dieser Daten zwischen den verknüpften Regionen und der Heimatregion. Updates, die in einer verknüpften Region auftreten, werden in die Heimatregion repliziert. Aktualisierungen, die in der Heimatregion vorgenommen werden, werden zurück in die verknüpfte Region repliziert. Wenn es in der Heimatregion und der verknüpften Region widersprüchliche Aktualisierungen gibt, wird das neueste Update verwendet.

Alle Ergebnisse, die in einer Region zu dem Zeitpunkt vorlagen, zu dem sie zu einer verknüpften Region wurde, werden nicht in die Heimatregion repliziert, es sei denn, die Ergebnisse werden aktualisiert. Nachdem eine Region mit einer Heimatregion verknüpft wurde, unterscheiden sich die Ergebnisse zwischen der Heimatregion und der verknüpften Region, bis die Ergebnisse in der verknüpften Region aktualisiert werden oder sie veralten.

Alle Ressourcen, die zu dem Zeitpunkt, zu dem sie eine verknüpfte Region wurde, in einer Region existierten, werden in die Heimatregion repliziert, in der Regel innerhalb von 24-48 Stunden, nachdem die Region mit einer Heimatregion verknüpft wurde.

Wenn eine verknüpfte Region entfernt wird, verbleiben alle Ergebnisse oder Ressourcen für diese Region in der Heimatregion, bis der Fund oder die Ressource veraltet ist.

Trenddaten basieren auf Erkenntnissen und Ressourcen, die in der Region vorhanden sind, für die der Trend bestimmt ist. Trenddaten in einer Heimatregion spiegeln den aktuellen Stand der Ergebnisse und Ressourcen wider, die mit der Heimatregion synchronisiert wurden.



Cross-Region Die Aggregation erhöht die Kosten von Security Hub nicht. Es fallen keine Gebühren an, wenn Security Hub neue Daten oder Updates repliziert.

In der Heimatregion bietet die Übersichtsseite einen Überblick über Ihre aktiven Ergebnisse und Ressourcen in den verknüpften Regionen.

Security Hub aggregiert nur Daten aus Regionen, in denen Security Hub für ein Konto aktiviert ist. Security Hub wird nicht automatisch für ein Konto aktiviert, das auf der regionsübergreifenden Aggregationskonfiguration basiert.

Es ist möglich, die regionsübergreifende Aggregation zu aktivieren, ohne dass verknüpfte Regionen ausgewählt werden. In diesem Fall findet keine Datenreplikation statt.

Aggregation für Administrator- und Mitgliedskonten

Eigenständige Konten und Administratorkonten können die regionsübergreifende Aggregation konfigurieren. Falls von einem Administrator konfiguriert, ist das Vorhandensein des Administratorkontos unerlässlich, damit die regionsübergreifende Aggregation in verwalteten Konten funktioniert. Wenn das Administratorkonto entfernt oder von einem Mitgliedskonto getrennt wird, wird die regionsübergreifende Aggregation für dieses Mitgliedskonto beendet. Wenn das Mitgliedskonto jedoch vor der Verknüpfung mit einem Administrator über eine eigene regionsübergreifende Aggregationskonfiguration verfügte, wird diese Konfiguration wieder wirksam.

Wenn ein Administratorkonto die regionsübergreifende Aggregation aktiviert, repliziert Security Hub die Daten, die das Administratorkonto in allen verknüpften Regionen generiert, in die Heimatregion. Darüber hinaus identifiziert Security Hub die Mitgliedskonten, die diesem Administrator zugeordnet sind, und jedes Mitgliedskonto erbt die regionsübergreifenden Aggregationseinstellungen des Administrators. Security Hub repliziert die Daten, die ein Mitgliedskonto in allen verknüpften Regionen generiert, in die Heimatregion.

Der Administrator kann von allen Mitgliedskonten in den verwalteten Regionen aus auf Sicherheitsergebnisse zugreifen und diese verwalten. Darüber hinaus kann der Administrator den Ressourcenbestand aller Mitgliedskonten in den verwalteten Regionen einsehen.

Als Security Hub-Mitgliedskonto müssen Sie in der Heimatregion angemeldet sein, um aggregierte Daten aus Ihrem Konto aus allen verknüpften Regionen einsehen zu können. Mitgliedskonten sind nicht berechtigt, Daten von anderen Mitgliedskonten einzusehen, und dürfen die `GetAggregatorV2` APIs `CreateAggregatorV2``DeleteAggregatorV2`, und nicht aufrufen.

Automatisierungsregeln und regionsübergreifende Aggregation

Wenn die regionsübergreifende Aggregation aktiviert ist, können Automatisierungsregeln nur in der definierten Heimatregion erstellt werden. Jede Regel, die Sie definieren, gilt für alle verknüpften Regionen, es sei denn, Ihre Regelkriterien gelten für bestimmte Regionen. Sie müssen separate Automatisierungsregeln für jede Region erstellen, die keine verknüpfte Region ist.

Alle Regeln, die vor der Aktivierung der regionsübergreifenden Aggregation in der Heimatregion erstellt wurden, gelten automatisch für verknüpfte Regionen. Regeln, die zuvor in verknüpften Regionen erstellt wurden, gelten nicht mehr, sobald ein Aggregator erstellt wurde. Regeln, die in verknüpften Regionen definiert wurden, gelten wieder, nachdem der Aggregator gelöscht wurde oder die Region nicht mehr verknüpft ist.

Aktivierung der regionsübergreifenden Aggregation

Sie müssen die regionsübergreifende Aggregation von der AWS Region aus aktivieren, die Sie als Heimatregion festlegen möchten.

Um die regionsübergreifende Aggregation zu aktivieren, erstellen Sie eine Security Hub Hub-Ressource, die als Finding-Aggregator bezeichnet wird. Die Suchaggregator-Ressource gibt Ihre Heimatregion und verknüpfte Regionen (falls vorhanden) an.

Sie können eine AWS Region, die standardmäßig deaktiviert ist, nicht als Heimatregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie in der AWS allgemeinen Referenz unter Region aktivieren.

Wenn Sie die regionsübergreifende Aggregation aktivieren, können Sie bei Bedarf eine oder mehrere verknüpfte Regionen angeben. Durch die Aktivierung der regionsübergreifenden Aggregation wird Security Hub in dieser Region nicht aktiviert. Informationen zur Aktivierung von Security Hub in einer Region finden Sie unter Erstellen einer Richtlinie als delegierter Administrator zur Verwaltung von Mitgliedskonten im Security Hub Hub-Benutzerhandbuch.

So aktivieren Sie die regionsübergreifende Aggregation (Konsole)

1. Öffnen Sie über das Administratorkonto oder in einem eigenständigen Konto die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home
2. Melden Sie sich mit der AWS Regionsauswahl bei der Region an, die Sie als Aggregationsregion verwenden möchten.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Allgemein.
4. Wählen Sie im Abschnitt Cross-Region Aggregation die Option Konfigurieren aus.
5. Standardmäßig ist die Heimatregion auf Keine Aggregationsregion eingestellt.
6. Wählen Sie unter Heimatregion die Option aus, um die aktuelle Region als Heimatregion festzulegen.
7. Wählen Sie optional für Verknüpfte Regionen die Regionen aus, aus denen Daten aggregiert werden sollen.
8. Wählen Sie Speichern.

Überprüfen der Einstellungen für die regionsübergreifende Aggregation

Sie können die aktuelle regionsübergreifende Aggregationskonfiguration in AWS Security Hub von jeder AWS Region aus im Administratorkonto oder in einem eigenständigen Konto anzeigen. Mitgliedskonten können die regionsübergreifende Aggregationskonfiguration nicht anzeigen. Die Konfiguration umfasst die Heimatregion und die verknüpften Regionen (falls vorhanden).

Folgen Sie den Schritten, um Ihre aktuellen regionsübergreifenden Aggregationseinstellungen anzuzeigen

So zeigen Sie die Einstellungen für die regionsübergreifende Aggregation an (Konsole)

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Allgemein aus.
3. Wenn die regionsübergreifende Aggregation nicht aktiviert ist, wird auf der Seite Allgemein die Option zur Aktivierung der regionsübergreifenden Aggregation angezeigt. Nur Administratorkonten und eigenständige Konten können die regionsübergreifende Aggregation aktivieren.
4. Wenn die regionsübergreifende Aggregation aktiviert ist, werden auf der Registerkarte Regionen die folgenden Informationen angezeigt:
   - Die Heimatregion
   - Ob Ergebnisse, Ressourcen und Trends aus neuen Regionen, die Security Hub unterstützt und für die Sie sich entscheiden, automatisch aggregiert werden sollen
   - Die Liste der verknüpften Regionen (falls ausgewählt)

Aktualisierung der regionsübergreifenden Aggregationseinstellungen

Sie können Ihre aktuellen regionsübergreifenden Aggregationseinstellungen in AWS Security Hub aktualisieren, indem Sie die verknüpften Regionen oder die aktuelle Heimatregion ändern.

Änderungen an der regionsübergreifenden Aggregation werden für eine Opt-in-Region erst implementiert, wenn Sie die Region in Ihrem Konto aktivieren. AWS Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, sind Opt-in-Regionen.

Wenn Sie die Aggregation von Daten aus einer verknüpften Region beenden, entfernt AWS Security Hub keine vorhandenen aggregierten Daten aus dieser Region, auf die in der Heimatregion zugegriffen werden kann.

Sie können die Aktualisierungsverfahren in diesem Abschnitt nicht verwenden, um die Heimatregion zu ändern. Um die Heimatregion zu ändern, müssen Sie wie folgt vorgehen:

1. Löschen Sie die aktuelle regionsübergreifende Aggregationskonfiguration. Detaillierte Anweisungen finden Sie unter the section called “Aggregation wird gelöscht”.
2. Wechseln Sie zu der Region, die Sie als neue Heimatregion verwenden möchten.
3. Aktivieren Sie die regionsübergreifende Aggregation. Detaillierte Anweisungen finden Sie unter the section called “Aggregation aktivieren”.

Sie müssen die regionsübergreifende Aggregationskonfiguration von der aktuellen Heimatregion aus aktualisieren.

Um die verknüpften Regionen zu ändern (Konsole)

1. Öffnen Sie über das Administratorkonto oder in einem eigenständigen Konto die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Melden Sie sich in der aktuellen Aggregationsregion an.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Allgemein.
4. Wählen Sie für Cross-Region die Aggregation Bearbeiten aus.
5. Aktualisieren Sie für verknüpfte Regionen die ausgewählten verknüpften Regionen.
6. Wählen Sie Speichern.

Regionsübergreifende Aggregation wird gelöscht

Wenn Sie nicht möchten, dass AWS Security Hub Daten aggregiert, können Sie Ihren Suchaggregator löschen. Alternativ können Sie Ihren Suchaggregator beibehalten, aber keine AWS Regionen mit der Heimatregion verknüpfen, indem Sie den vorhandenen Aggregator so aktualisieren, dass keine verknüpften Regionen ausgewählt sind.

Um Ihre Heimatregion zu ändern, müssen Sie Ihren aktuellen Suchaggregator löschen und einen neuen erstellen.

Wenn Sie Ihren Suchaggregator löschen, beendet Security Hub die Datenaggregation. Es entfernt keine vorhandenen aggregierten Daten aus der Heimatregion.

Der Suchaggregator (Konsole) wird gelöscht

Sie können Ihren Suchaggregator nur aus der aktuellen Heimatregion löschen.

In anderen Regionen als der Heimatregion wird im Bereich Finding Aggregation auf der Security Hub Hub-Konsole eine Meldung angezeigt, dass Sie die Konfiguration in der Heimatregion bearbeiten müssen. Wählen Sie diese Nachricht, um einen Link anzuzeigen, über den Sie zur Heimatregion wechseln können.

Um die regionsübergreifende Aggregation zu beenden (Konsole)

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Stellen Sie sicher, dass Sie in Ihrer aktuellen Heimatregion angemeldet sind.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Allgemein.
4. Wählen Sie unter Cross-Region Aggregation die Option Bearbeiten aus.
5. Wählen Sie unter Aggregationsregion die Option Keine Aggregationsregion aus.
6. Wählen Sie Speichern.
7. Geben Sie im Bestätigungsdialogfeld in das Bestätigungsfeld Folgendes ein. **`Confirm`**
8. Wählen Sie Bestätigen aus.

Integration von Security Hub mit Microsoft Azure

Um Ihre Microsoft Azure-Ressourcen zu überwachen, können Sie Microsoft Azure in AWS Security Hub integrieren. Security Hub aktiviert dann automatisch das Statusmanagement und das Schwachstellenmanagement für Ihre Azure-Umgebung und generiert Ergebnisse und andere Daten über Ihre Umgebung. Sie müssen keine Azure-Sicherheitsdienste aktivieren — alle Funktionen werden von ausgeführt. AWS Genauer gesagt bietet Ihnen der Dienst Folgendes:

CIS Microsoft Azure Foundations Benchmark v4.0 und Azure Foundational Best Practices

> Automatisierte Konformitätsprüfungen anhand des CIS Azure v4.0-Standards und des Azure Foundational Best Practices-Standards. Diese Standards decken Identitäts-, Netzwerk-, Speicher-, Protokollierungs- und Datenbankkontrollen ab.

Schwachstellenmanagement

Amazon Inspector scannt Ihre Azure-VMs, Function Apps und Azure Container Registry (ACR) -Container-Images automatisch über den serviceverknüpften Connector auf Software-Sicherheitslücken.

> **Note**
>
> Für das Scannen virtueller Maschinen muss Amazon EC2 Systems Manager in derselben Region konfiguriert sein. Einzelheiten zur Einrichtung finden Sie in der Amazon Inspector-Dokumentation zur Azure-Integration.

Korrelation der Exposition

Automatisierte Erkennung exponierter Azure-Ressourcen auf der Grundlage von Kombinationen aus Netzwerkerreichbarkeit, öffentlichem Zugriff und Fehlkonfigurationen.

Warnmeldungen zur Erkennung von Bedrohungen durch Microsoft Defender for Cloud

Wenn Sie den kontinuierlichen Export von Azure Defender in den Event Hub konfigurieren, nimmt Security Hub Defender for Cloud-Warnmeldungen zur Bedrohungserkennung auf und ordnet sie dem Format Open Cybersecurity Schema Framework (OCSF) zu. Diese werden zusammen mit Ihrem Statusmanagement und Ihren Sicherheitslücken in der Security Hub-Konsole angezeigt.

Inventar der Vermögenswerte

Ein vollständiges Inventar Ihrer Azure-Ressourcen, das durch die Integration erkannt wurde und in der Security Hub-Konsole zusammen mit Ihren AWS Ressourcen angezeigt wird.

OCSF-Format

Security Hub generiert alle Ergebnisse im Format des Open Cybersecurity Schema Framework (OCSF) AWS und bietet so ein einheitliches Schema für alle Azure-Ergebnisse.

Um die Integration zu erstellen, verbinden Sie Ihre Azure-Umgebung wie folgt mit Security Hub:

1. Sie konfigurieren Ihre Azure-Umgebung mit einer Anwendungsregistrierung, Verbundidentitätsdaten, Azure-Rollenzuweisungen und einer Event Hub-Infrastruktur.
2. Mithilfe der Security Hub-Konsole erstellen Sie einen Connector für die Integration. Sie geben Ihre Azure-Mandanten-ID, die Anwendungsclient-ID, den Überwachungsumfang und die Event Hub-Region an.

3. Security Hub erstellt die erforderlichen dienstbezogenen Rollen und Ressourcen in Ihrem AWS-Konto.
4. AWS Config sammelt Ressourcenkonfigurationsdaten aus Ihrer Azure-Umgebung.

   AWS Config wird intern verwendet, um Ressourcenkonfigurationsdaten zu sammeln. Im Gegensatz AWS zur Statusverwaltung, bei der Sie die Aufzeichnung explizit aktivieren AWS Config und dafür bezahlen müssen, erfolgt die Azure-Statusverwaltung AWS Config automatisch. Sie müssen den Rekorder nicht AWS Config separat aktivieren, keinen Rekorder konfigurieren oder für die AWS Config Nutzung separat bezahlen. Diese Kosten sind in Ihrem Security Hub-Preis enthalten.
5. Security Hub empfängt ab sofort Ressourcenkonfigurationsdaten und Aktivitätsprotokollereignisse aus Ihrer Azure-Umgebung.
6. Security Hub generiert Informationen zur Statusverwaltung und zu Sicherheitslücken in Ihrer Azure-Umgebung.

Wie AWS Config wird verwendet

AWS Config wird intern verwendet, um Ressourcenkonfigurationsdaten zu sammeln und Änderungen in Ihrer Azure-Umgebung zu erkennen. Der Connector verarbeitet dies automatisch. Sie müssen den Rekorder nicht AWS Config separat aktivieren, keinen Rekorder konfigurieren oder für die AWS Config Nutzung bezahlen. Diese Kosten sind in Ihrem Security Hub-Preis für Azure-Ressourcen enthalten.

Zusätzliche Informationen

Wenn Sie die Integration erstellen, erstellt Security Hub automatisch auch entsprechende dienstbezogene Integrationen in Security Hub CSPM und Amazon Inspector. Diese servicetechnischen Integrationen stellen sicher, dass der Umfang Ihrer CSPM-Prüfungen und Ihrer Inspector-Schwachstellenscans dem Umfang entspricht, den Sie in Security Hub definieren. Wenn Sie den Umfang ändern möchten, müssen Sie die Änderungen im Security Hub vornehmen. Sie können eine dienstgebundene Integration nicht direkt in Security Hub CSPM oder Inspector ändern.

Sie können eine Azure-Integration auch direkt in Security Hub CSPM erstellen und unabhängige Bereichseinstellungen angeben. Die CSPM-Integration funktioniert dann unabhängig von der Security Hub-Integration und kann einen unterschiedlichen Geltungsbereich für das Azure-Abonnement und die Azure-Region haben.

Informationen zur Schätzung und Berechnung der Kosten für die Integration von Security Hub in Azure finden Sie unter AWS Security Hub-Preise.

Themen

- Voraussetzungen für die Integration von Security Hub mit Microsoft Azure
- Konfiguration von Microsoft Azure für die Integration mit Security Hub
- Konfiguration von Security Hub für die Integration mit Microsoft Azure
- Löschen eines Microsoft Azure-Connectors in Security Hub

Voraussetzungen für die Integration von Security Hub mit Microsoft Azure

Bevor Sie Microsoft Azure in AWS Security Hub integrieren, führen Sie die folgenden Aufgaben in Ihrer AWS und Azure-Umgebung aus. Dadurch wird sichergestellt, dass Sie und Security Hub über die Ressourcen und Berechtigungen verfügen, die Sie zur Überwachung Ihrer Azure-Ressourcen benötigen.

Themen

- Voraussetzungen für AWS
- Voraussetzungen für Microsoft Azure

Voraussetzungen für AWS

Stellen Sie sicher, dass Sie Folgendes in Ihrem haben AWS-Konto:

AWS Security Hub aktiviert

Security Hub muss in dem AWS-Konto und in AWS-Region dem Sie den Connector erstellen möchten, aktiviert sein. Sie müssen Security Hub aktivieren, bevor Sie einen Azure-Connector erstellen.

AWS Security Hub CSPM ist aktiviert

Security Hub CSPM muss im selben Land aktiviert sein. AWS-Konto AWS-Region Die Azure-Integration stützt sich auf Security Hub CSPM für die Bewertung der Ressourcenkonfiguration.

IAM-Berechtigungen für die Konsole

Der IAM-Prinzipal, der den Connector erstellt, muss über die folgenden Berechtigungen verfügen:

- `config:GetConnector`

- `config:ListConnectors`
- `config:PutConnector`

IAM Outbound Identity Federation ist aktiviert

Sie müssen IAM Outbound Identity Federation in Ihrem aktivieren. AWS-Konto Diese Funktion ermöglicht es AWS Diensten, sich bei externen Identitätsanbietern (wie Microsoft Entra ID) zu authentifizieren, indem sie Verbundanmeldeinformationen anstelle von langlebigen Geheimnissen verwenden.

Nachdem Sie den Outbound Identity Federation aktiviert haben, notieren Sie sich die URL des Token-Ausstellers. Diese URL folgt dem Format:

```
https://uuid.tokens.sts.global.api.aws
```

Sie benötigen diese URL, wenn Sie Anmeldeinformationen für Verbundidentitäten in Azure konfigurieren.

Voraussetzungen für Microsoft Azure

Stellen Sie sicher, dass in Ihrer Azure-Umgebung Folgendes vorhanden ist:

Azure-Mandant

Sie müssen einen Azure-Mandanten in der kommerziellen Azure-Cloud haben. Azure Government und Azure China werden nicht unterstützt.

Verfügbarkeit des Microsoft Entra ID-Protokolls

Für die Ressourcenaufzeichnung sind Microsoft Graph-Auditprotokolle und Anmeldeprotokolle von Ihrem Microsoft Entra ID-Mandanten erforderlich. Für einige Microsoft Entra ID-Protokolle ist eine Microsoft Entra ID P1- oder P2-Lizenz erforderlich.

Wenn dem Mandanten die erforderlichen Protokolle fehlen, werden bei der Ressourcenaufzeichnung möglicherweise Teilfehler gemeldet. Die App-Registrierung und die Azure-Rollenzuweisungen liefern keine fehlenden Protokolldaten.

Rolle des globalen Administrators

Sie müssen über die Rolle des globalen Administrators in Microsoft Entra ID verfügen, um die Azure-Umgebung konfigurieren zu können. Diese Rolle ist erforderlich, um Anwendungen zu

registrieren, die Zustimmung des Administrators für Microsoft Graph-API-Berechtigungen zu erteilen, RBAC-Rollen im Bereich der Mandantenstammverwaltungsgruppe zuzuweisen und Diagnoseeinstellungen für Entra-ID-Auditprotokolle zu konfigurieren.

Zusätzlich zu Global Administrator benötigen Sie die folgenden Azure RBAC-Rollen, um die Ressourcen zu erstellen, die für die Integration erforderlich sind:

- Benutzerzugriffsadministrator (oder Besitzer) im Stammbereich (/) — um RBAC-Rollen im Bereich der Stammverwaltungsgruppe des Mandanten zuzuweisen.
- Resource Policy Contributor (oder Besitzer) im Bereich der Stammverwaltungsgruppe des Mandanten — zur Erstellung der Azure-Richtliniendefinitionen und -zuweisungen, mit denen Diagnoseeinstellungen und Problembehebungen automatisiert werden.
- Mitwirkender (oder Eigentümer) im Abonnementbereich, der den Event Hub hostet — um den Event Hub-Namespace und die zugehörigen Ressourcen zu erstellen.

> **Note**
>
> In vielen Organisationen sind der globale Azure-Administrator und der AWS Sicherheitsadministrator unterschiedliche Personen. Das Azure-Setup kann mithilfe des generierten Setup-Skripts unabhängig abgeschlossen werden.

Nachdem Sie diese Aufgaben abgeschlossen haben, können Sie Ihre Azure-Umgebung konfigurieren.

Konfiguration von Microsoft Azure für die Integration mit Security Hub

Nachdem Sie die erforderlichen Aufgaben abgeschlossen haben, können Sie Ihre Microsoft Azure-Umgebung so konfigurieren, dass die Integration mit AWS Security Hub unterstützt wird. Um Ihnen dabei zu helfen, generiert die Security Hub-Konsole ein Setup-Skript, das auf Ihre Konfiguration zugeschnitten ist.

Um das Setup-Skript zu generieren

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie Create Azure Connector.

4. Vervollständigen Sie die Connector-Konfiguration (Mandanten-ID, Bereich und Name) und kopieren Sie dann das generierte Setup-Skript.

Um das Skript auszuführen, verwenden Sie die Azure-CLI und authentifizieren Sie sich mit einem globalen Administratorkonto (`az login`).

Wenn Sie das Skript ausführen, führt es eine Reihe von Aufgaben aus. In den folgenden Abschnitten wird jede Aufgabe beschrieben, die das Skript ausführt. Wenn Ihre Organisation die Ausführung von Skripten einschränkt, können Sie diese Aufgaben manuell ausführen, indem Sie dieses Thema als Leitfaden verwenden. Nachdem Sie Ihre Azure-Umgebung konfiguriert haben, können Sie Security Hub für die Integration in Azure ??? konfigurieren.

In den Schritten 1—7 wird die gemeinsame Grundlage konfiguriert, auf der alle Security Hub-Funktionen basieren: Anwendungsregistrierung, Verbundanmeldeinformationen, Azure-Rollenzuweisungen, Microsoft Graph-Berechtigungen, Event Hub und Protokollexport. In den Schritten 8—10 werden die zusätzlichen Azure-Ressourcen für bestimmte Funktionen konfiguriert:

- Schwachstellenmanagement (Amazon Inspector) — Konfiguriert den Export von Repository-Ereignissen in Azure Container Registry (ACR) und eine vom System zugewiesene verwaltete Identität auf Ihren Azure-VMs.
- Bedrohungserkennung (Microsoft Defender for Cloud) — Konfiguriert Microsoft Defender for Cloud so, dass Sicherheitswarnungen kontinuierlich in den Event Hub exportiert werden.

> **Note**
>
> Eine einzige Azure-App-Registrierung wird von allen AWS Sicherheitsdiensten gemeinsam genutzt. Wenn Sie auch Security Hub CSPM oder Amazon Inspector for Azure verwenden, verwenden diese dieselbe App-Registrierung. Sie müssen nicht für jeden AWS Dienst separate Registrierungen erstellen.

Aufgaben

- Schritt 1: Registrieren Sie eine Azure-Anwendung
- Schritt 2: Erstellen Sie einen Service Principal
- Schritt 3: Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität
- Schritt 4: Weisen Sie RBAC-Rollen zu

- Schritt 5: Konfigurieren Sie die Microsoft Graph API-Berechtigungen
- Schritt 6: Azure Event Hub einrichten
- Schritt 7: Konfigurieren Sie das Aktivitätsprotokoll und den Export des Entra ID-Auditprotokolls
- Schritt 8: Konfigurieren Sie den Azure Container Registry-Export
- Schritt 9: Aktivieren Sie eine verwaltete Identität auf Azure-VMs
- Schritt 10: Microsoft Defender for Cloud-Benachrichtigungen exportieren

Schritt 1: Registrieren Sie eine Azure-Anwendung

Registrieren Sie eine neue Anwendung in Microsoft Entra ID. Diese Anwendung dient als Identität, die zur Authentifizierung in Ihrer Azure-Umgebung mithilfe von Verbundanmeldeinformationen AWS verwendet wird. Es sind keine Client-Geheimnisse erforderlich.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Notieren Sie sich die Anwendungs-ID (Client) aus der Ausgabe (das `appId` Attribut). Sie geben diesen Wert an, wenn Sie den Connector in der Security Hub-Konsole erstellen.

Schritt 2: Erstellen Sie einen Service Principal

Erstellen Sie einen Dienstprinzipal für die registrierte Anwendung. Sie verwenden Azure-Rollenzuweisungen, um dem Dienstprinzipal Berechtigungen zu erteilen. Der Dienstprinzipal führt Aktionen in Ihrer Azure-Umgebung durch.

```
$ az ad sp create --id application-client-id
```

Wo *`application-client-id`* ist die Anwendungs-ID (Client) aus dem vorherigen Schritt.

Stellen Sie die Anwendungs-ID-URI bei der Registrierung auf ein`api://`*`application-client-id`*. AWS benötigt diese Kennung, um Verbund-Token mit der Anwendung auszutauschen. Ohne diesen URI AWS kann keine gültige Zielgruppe für Verbund-Tokens generiert werden, und jede Funktion kann sich nicht bei Azure authentifizieren.

```
$ az ad app update \
  --id application-client-id \
  --identifier-uris "api://application-client-id"
```

Schritt 3: Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität

Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität in der Anwendung, um eine Authentifizierung ohne AWS geheime Client-Schlüssel zu ermöglichen. Dadurch wird eine OIDC-Vertrauensstellung zwischen und Azure hergestellt. AWS Es werden keine langlebigen Geheimnisse oder Anmeldeinformationen gespeichert.

Die Security Hub Azure-Integration authentifiziert sich mithilfe einer AWS IAM-Rolle pro Funktion: Erkennung der Ressourcenkonfiguration, Schwachstellenmanagement und Bedrohungserkennung. Fügen Sie für jede Rolle einen Identitätsverbund hinzu, sodass sich jede Funktion bei Azure authentifizieren kann. AWS erstellt die dienstverknüpften Rollen automatisch, wenn Sie den Connector erstellen. Die für das VM-Scannen `Inspector2SSMFederationRole` verwendete Rolle ist keine serviceverknüpfte Rolle. Sie erstellen sie als Teil der Amazon Inspector VM-Scaneinrichtung, wie in Schritt 9 beschrieben.

Funktion	Betreff (IAM-Rollen-ARN)
Erkennung der Ressourcenkonfiguration ()AWS Config	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty`
Schwachstellenmanagement (Inspector)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdParty`
Schwachstellenmanagement — VM-Scannen (Amazon EC2 Systems Manager)	`arn:aws:iam::` *`account-id`* `:role/Inspector2SSMFederationRole-` *`tenant-id`*
Erkennung von Bedrohungen (Security Hub)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/securityhubv2.amazonaws.com/AWSServiceRoleForSecurityHubV2`

Führen Sie den folgenden Befehl einmal für jeden Betreff in der obigen Tabelle aus, `name` und ändern Sie dabei jedes Mal die `subject` Werte und. Die `audiences` Werte `issuer` und sind für alle Anmeldeinformationen identisch.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "credential-name",
    "issuer": "token-issuer-url",
    "subject": "service-linked-role-arn",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "AWS federation for Security Hub Azure integration"
  }'
```

Die wichtigsten Werte:

- Aussteller — Ihre Token-Aussteller-URL von IAM Outbound Identity Federation. Dies folgt dem Format. `https://uuid.tokens.sts.global.api.aws`
- Betreff — Ein IAM-Rollen-ARN aus der vorherigen Tabelle. Die Rolle *`tenant-id`* in der Amazon EC2 Systems Manager-Rolle ist Ihre Azure-Mandanten-ID.
- Zielgruppe — `api://AzureADTokenExchange` (Standardwert für den Workload-Identitätsverbund).
- Name — Jeder Name, der innerhalb der Anwendung eindeutig ist.

Schritt 4: Weisen Sie RBAC-Rollen zu

Weisen Sie dem Service Principal die folgenden integrierten Rollen zu:

- Reader — Gewährt schreibgeschützten Zugriff auf alle Azure-Ressourcen, sodass Security Hub Ihre Ressourcenkonfigurationen erkennen und auswerten kann. Weisen Sie diese Rolle im Stammbereich zu ()/.
- Mitwirkender — Gewährt den Schreibzugriff, den Amazon Inspector benötigt, um Ihre virtuellen Azure-Computer, Function Apps und Container-Images auf Sicherheitslücken zu scannen. Weisen Sie diese Rolle im Bereich der Stammverwaltungsgruppe des Mandanten zu, wodurch sie auf jedes Abonnement im Mandanten übertragen wird.
- Azure Event Hubs Data Receiver — Ermöglicht AWS das Lesen von Ereignissen aus dem Event Hub. Weisen Sie diese Rolle im Bereich der Stammverwaltungsgruppe des Mandanten zu.

⚠ Weisen Sie Reader im Stammbereich zu

Stellen Sie sicher, dass Sie die Reader-Rolle im Stammbereich (/) zuweisen, nicht im Bereich der Mandanten-Stammverwaltungsgruppe. Security Hub liest Azure-Ressourcen für die Rollenzuweisung in jedem Bereich, einschließlich Aufgaben, die sich auf das Stammverzeichnis des Mandanten beziehen. Eine Leserzuweisung in der Stammverwaltungsgruppe deckt keine Aufgaben ab/, deren Geltungsbereich darin liegt. Andernfalls schlagen diese Lesevorgänge mit einem Autorisierungsfehler fehl und der Connector kann in einen herabgesetzten Zustand übergehen.

⚠ Der Mitwirkende gewährt mandantenweiten Schreibzugriff

Die Rolle „Mitwirkender“ im Bereich der Stammverwaltungsgruppe für Mandanten gewährt hochprivilegierten, mandantenweiten Schreibzugriff auf Ihre Azure-Ressourcen. Security Hub benötigt diesen Zugriff, damit Amazon Inspector Ihre Rechenressourcen nach Sicherheitslücken durchsuchen kann. Beispielsweise verwendet Inspector die von Contributor bereitgestellten Ausführungsbefehle für virtuelle Maschinen. Über Amazon EC2 Systems Manager Automation führt Inspector Befehle auf Ihren Azure-VMs aus, um den VM Scanner-Agenten zu installieren und zu betreiben.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Contributor" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope Für die Zuweisung sind erweiterte Zugriffsrechte erforderlich

Für die Zuweisung einer Rolle im Stammbereich (/) sind erhöhte Zugriffsrechte erforderlich. Wenn eine Rollenzuweisung fehlschlägt, stellen Sie sicher, dass die Zugriffsverwaltung für Azure-Ressourcen unter Microsoft Entra ID > Eigenschaften auf Ja gesetzt ist. Melden Sie sich dann ab und wieder an, um Ihr Token zu aktualisieren.

Entfernen Sie die temporäre Wurzelhöhe

Wenn Sie die Zugriffsverwaltung für Azure-Ressourcen aktivieren, wird dem angemeldeten Administrator die Rolle des Benutzerzugriffsadministrators im Stammbereich (/) zugewiesen, der den Zugriff für jedes Abonnement und jede Verwaltungsgruppe im Mandanten verwalten kann. Wenn das Onboarding abgeschlossen ist, setzen Sie die Zugriffsverwaltung für Azure-Ressourcen unter Microsoft Entra ID > Eigenschaften wieder auf Nein, speichern Sie und melden Sie sich ab, damit diese Erhöhung nicht aktiv bleibt.

Schritt 5: Konfigurieren Sie die Microsoft Graph API-Berechtigungen

Erteilen Sie der Anwendung die folgenden Microsoft Graph API-Berechtigungen (Anwendungstyp) und erteilen Sie dann die Zustimmung des Administrators:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Schritt 6: Azure Event Hub einrichten

AWS Config verwendet einen Azure Event Hub, um nahezu in Echtzeit Benachrichtigungen über Änderungen der Ressourcenkonfiguration in Ihrer Azure-Umgebung zu erhalten. Das Setup-Skript erstellt die Event Hub-Infrastruktur und markiert sie zur Erkennung. Die Event Hub-Erkennung verwendet eine tagbasierte Auflösung: Security Hub sucht im Event Hub-Namespace nach einem Tag mit dem Format, `AWSConfig-account-id-region` um die richtige Event Hub-Instanz für Ihre Integration zu identifizieren.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Nachdem Sie den Event Hub erstellt haben, kennzeichnen Sie den Namespace für die Erkennung und weisen Sie die Rolle des Datenempfängers zu. Verwenden Sie `az tag update` with, `--operation merge` um alle anderen Tags im Namespace beizubehalten (z. B. das Discovery-Tag zur Erkennung von Bedrohungen aus Schritt 10):

```
$ az tag update \
```

```
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> *account-id*Ist im Tag-Format Ihre 12-stellige AWS-Konto ID und *region* der OrtAWSConfig-*account-id*-*region*, AWS-Region an dem Sie den Connector erstellen (z. B.us-east-1). Diese Werte geben an, welcher AWS-Konto und welcher Region diese Event Hub-Integration gehört.

Wichtige Konfiguration:

- Namespace-SKU — Standard (für Verbrauchergruppen erforderlich).
- Name des Event Hubs —activitylog.
- Verbrauchergruppe —AWSConfig.
- Tag — AWSConfig-*account-id*-*region* mit Wertactivitylog. Dieses Tag ermöglicht es AWS Config , den Event Hub automatisch zu erkennen.
- Rollenzuweisung — Azure Event Hubs Data Receiver im Namespace.

Zur Bedrohungserkennung erstellt das Setup außerdem einen separaten defender-alerts Event Hub mit einer Benutzergruppe und AWSSecurityHub fügt ein zweites Discovery-Tag in dem Format hinzu, das den Hub identifiziertAWSSecurityHub-*account-id*-*region*, den Security Hub direkt liest. Weitere Informationen finden Sie in Schritt 10.

Schritt 7: Konfigurieren Sie das Aktivitätsprotokoll und den Export des Entra ID-Auditprotokolls

Konfigurieren Sie Azure so, dass Aktivitätsprotokolle und Microsoft Entra ID-Protokolle in den Event Hub exportiert werden.

Export des Aktivitätsprotokolls:

Konfigurieren Sie die Diagnoseeinstellungen für jedes Abonnement, um Aktivitätsprotokolle in den Event Hub zu exportieren. Das Setup-Skript konfiguriert dies automatisch für alle überwachten Abonnements. Aktivitätsprotokolle erfassen Aktivitäten auf Abonnementebene, einschließlich Rollenzuweisungen und Ressourcenänderungen.

Export des Microsoft Entra ID-Protokolls:

Konfigurieren Sie die Diagnoseeinstellungen auf der Microsoft Entra ID, um Protokolle in denselben Event Hub zu exportieren. Navigieren Sie zu Microsoft Entra ID > Überwachung > Diagnoseeinstellungen > Diagnoseeinstellung hinzufügen. Aktivieren Sie AuditLogs SignInLogs, und NonInteractiveUserSignInLogs, und leiten Sie sie an Ihren Event Hub weiter.

Schritt 8: Konfigurieren Sie den Azure Container Registry-Export

Security Hub scannt Ihre Container-Images in Azure Container Registry (ACR) mithilfe von Amazon Inspector auf Sicherheitslücken. Dazu benötigt Inspector ACR-Repository-Ereignisse, die in einen Event Hub in derselben Azure-Region wie die Registrierung exportiert werden. Informationen zur Einrichtung des ACR-Exports finden Sie unter Konfiguration von Amazon Inspector für die Integration mit Microsoft Azure im Amazon Inspector-Benutzerhandbuch.

Schritt 9: Aktivieren Sie eine verwaltete Identität auf Azure-VMs

Security Hub scannt Ihre virtuellen Azure-Maschinen über Inspector. Für jede Azure-Ziel-VM muss eine vom System zugewiesene verwaltete Identität aktiviert sein. Um Ihren VMs diese Identität automatisch hinzuzufügen, weisen Sie zwei Azure-Richtlinien zu, die den `modify` Effekt im Bereich der Stammverwaltungsgruppe für Mandanten nutzen:

- Für eine virtuelle Maschine ohne Identität fügt die Richtlinie eine vom System zugewiesene verwaltete Identität hinzu.
- Für eine virtuelle Maschine, die nur über eine vom Benutzer zugewiesene Identität verfügt, fügt die Richtlinie eine vom System zugewiesene verwaltete Identität hinzu, wobei die vorhandenen, vom Benutzer zugewiesenen Identitäten beibehalten werden.

Eine virtuelle Maschine, die bereits über eine vom System zugewiesene verwaltete Identität verfügt, bleibt unverändert. Da die Richtlinien den `modify` Effekt nutzen, passen sie die bestehende Identität an, ohne die VM erneut bereitzustellen.

Inspector verwendet Amazon EC2 Systems Manager Automation, um den Inspector VM Scanner-Agenten auf Ihren Azure-VMs bereitzustellen und zu verwalten. Dies erfordert eine zusätzliche

Einrichtung AWS auf der Seite, einschließlich eines IAM-OIDC-Identitätsanbieters für Microsoft Entra ID und mehrerer IAM-Rollen. Die vollständige Einrichtung des VM-Scannens finden Sie unter Konfiguration von Amazon Inspector für die Integration mit Microsoft Azure im Amazon Inspector-Benutzerhandbuch.

Schritt 10: Microsoft Defender for Cloud-Benachrichtigungen exportieren

Security Hub nimmt Microsoft Defender for Cloud-Warnmeldungen zur Bedrohungserkennung auf und ordnet sie dem Open Cybersecurity Schema Framework (OCSF) -Format zu. Um diese Warnungen auszusenden, erstellen Sie einen speziellen `defender-alerts` Event Hub und konfigurieren Sie Microsoft Defender for Cloud so, dass kontinuierlich Sicherheitswarnungen dorthin exportiert werden.

Erstellen Sie im Event Hub-Namespace aus Schritt 6 den `defender-alerts` Event Hub, eine `AWSSecurityHub` Benutzergruppe, aus der Security Hub lesen kann, und eine Hub-spezifische SAS-Autorisierungsregel (Shared Access Signature) mit Sendeberechtigung, die Microsoft Defender for Cloud zum Senden von Warnmeldungen verwendet:

```
$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "defender-alerts" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "AWSSecurityHub"

$ az eventhubs eventhub authorization-rule create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "DefenderExportSend" \
  --rights Send
```

Fügen Sie dann ein zweites Discovery-Tag mit dem Namespace zusammen, sodass Security Hub den Hub erkennt. `defender-alerts` Verwenden Sie `az tag update` with, `--operation merge` um das `AWSConfig` Discovery-Tag aus Schritt 6 beizubehalten:

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSSecurityHub-account-id-region=defender-alerts"
```

Konfigurieren Sie abschließend den kontinuierlichen Export des Datentyps Sicherheitswarnungen durch Microsoft Defender for Cloud in den `defender-alerts` Event Hub. Gehen Sie im Azure-Portal zu Microsoft Defender for Cloud > Umgebungseinstellungen, wählen Sie das Abonnement aus, wählen Sie Kontinuierlicher Export > Event Hub, wählen Sie Sicherheitswarnungen und wählen Sie den `defender-alerts` Event Hub und die `DefenderExportSend` SAS-Regel aus.

> **Note**
>
> Wenn Sie den kontinuierlichen Export programmgesteuert (über die Azure Resource Manager-API, eine ARM-Vorlage oder Azure Policy) und nicht im Portal konfigurieren, authentifizieren Sie den Export zum Event Hub mit der `DefenderExportSend` SAS-Verbindungszeichenfolge. Rufen Sie es mit `az eventhubs eventhub authorization-rule keys list` für die `DefenderExportSend` Regel ab und legen Sie es als Verbindungszeichenfolge der Exportaktion fest. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Kontinuierlichen Export einrichten.

> **Note**
>
> Warten Sie nach Abschluss dieser Aufgaben etwa 15—30 Minuten, bis die Konfiguration wirksam wird. Stellen Sie dann sicher, dass Ihr Event Hub Nachrichten (die IncomingMessages Metrik) empfängt, bevor Sie den Connector in Security Hub erstellen.

Konfiguration von Security Hub für die Integration mit Microsoft Azure

Nachdem Sie die erforderlichen Aufgaben abgeschlossen und Ihre Microsoft Azure-Umgebung konfiguriert haben, können Sie AWS Security Hub für die Integration mit Azure konfigurieren. Um Security Hub für die Integration mit Azure zu konfigurieren, erstellen Sie einen Connector. Sie können den Connector von einem delegierten Administratorkonto oder dem Verwaltungskonto aus erstellen. Nachdem Sie den Connector erstellt haben, treten die folgenden Ereignisse auf:

1. Security Hub validiert die Azure-Anmeldeinformationen und die Konnektivität zu Ihrer Azure-Umgebung. Dieser Vorgang kann einige Minuten dauern.
2. Security Hub erstellt serviceverknüpfte Konnektoren in Security Hub CSPM und Amazon Inspector. Diese Konnektoren stellen sicher, dass Posture Management-Checks und Schwachstellenscans dem Umfang entsprechen, den Sie in Security Hub definiert haben.
3. AWS Config beginnt mit der Erkennung von Azure-Ressourcen mithilfe der föderierten Identitätsanmeldedaten.
4. Security Hub aktiviert automatisch den CIS Microsoft Azure Foundations Benchmark v4.0-Standard und den Azure Foundational Best Practices-Standard in CSPM für Ihre Azure-Ressourcen.
5. Erste Ergebnisse für Ressourcen mit Aktivitätsprotokollereignissen werden innerhalb von 15 bis 30 Minuten angezeigt. Die vollständige Bewertung aller vorhandenen Ressourcen kann bis zu 24 Stunden dauern.

Themen

- Erstellen Sie einen Azure-Connector
- Passen Sie den Umfang eines Azure-Connectors an
- Überprüfen Sie den Zustand eines Azure-Connectors
- Problembehandlung bei einem Azure-Connector
- Wie Security Hub mit Ressourcen umgeht und Identifikatoren findet

Erstellen Sie einen Azure-Connector

Um einen Microsoft Azure-Connector für Ihre Umgebung zu erstellen, führen Sie die folgenden Schritte mithilfe der AWS Security Hub Hub-Konsole oder der API aus.

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/advanced/home? region=us-ost-1. .
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie Azure-Konnektor erstellen.
4. Wählen Sie im Abschnitt Sicherheitsfunktionen aus, ob die Netzwerkscanfunktion aktiviert werden soll. Diese Funktion ist standardmäßig für das Konto aktiviert, für das Sie die Azure-Integration aktivieren, und kann deaktiviert werden, bevor Sie die Connector-Setup abschließen.

Wenn eine Organisationsrichtlinie diese Funktion für Ihr Konto blockiert, wird sie nicht als Option angezeigt. Weitere Informationen finden Sie unter Netzwerkscans in Security Hub.

5. Geben Sie für Azure Tenant ID Ihre Microsoft Entra ID-Mandanten-ID ein. Sie finden diese im Azure-Portal unter Microsoft Entra ID > Properties > Tenant ID.
6. Geben Sie unter Anwendungs-ID (Client) die Anwendungs-ID für die Azure-Anwendung ein, die Sie bei der Einrichtung der Azure-Umgebung registriert haben.
7. Konfigurieren Sie zusätzliche Einstellungen und den Umfang des Connectors, indem Sie wie folgt vorgehen:

   - Geben Sie unter Name einen eindeutigen Namen für den Connector ein. Der Name kann bis zu 50 alphanumerische Zeichen und Bindestriche enthalten.

     > **Note**
     >
     > Der Connectorname kann nach der Erstellung nicht geändert werden.

   - Geben Sie unter Beschreibung optional eine kurze Beschreibung des Connectors ein. Die Beschreibung kann bis zu 200 Zeichen enthalten.

     > **Important**
     >
     > Namen und Beschreibungen werden verwendet, um Ihre Inhalte zu identifizieren. Nehmen Sie keine sensiblen, vertraulichen oder persönlich identifizierbaren Informationen (PII) in sie auf.

   - Wählen Sie für Abonnements Alle Abonnements aus, um alle aktuellen und future Abonnements im Mandanten zu überwachen, oder Spezifische Abonnements, um nur die von Ihnen angegebenen Abonnements zu überwachen. Wenn Sie nur bestimmte Abonnements überwachen möchten, geben Sie die ID für jedes Abonnement ein.
   - Wählen Sie für Regionen die Option Alle Regionen aus, um Ressourcen in allen Azure-Regionen zu überwachen, oder Spezifische Regionen, um nur die von Ihnen angegebenen Regionen zu überwachen.

> **Note**
>
> Wenn Sie bereits einen Connector in Security Hub CSPM oder Amazon Inspector für denselben Azure-Mandanten erstellt haben, muss der Geltungsbereich des Connectors in Security Hub dieselben Abonnements und Regionen enthalten wie der Connector in Security Hub CSPM oder Amazon Inspector.

> **Note**
>
> Für Kontrollen, die Microsoft Entra ID- und Microsoft Graph-Ressourcen auswerten, muss der globale Bereich Region in Ihrer Integrationskonfiguration enthalten sein. Wenn Sie nur bestimmte Azure-Regionen auswählen, führen diese Kontrollen nicht zu Ergebnissen.

8. Überprüfen Sie die Konnektorkonfiguration.

> **Note**
>
> Wenn Sie Amazon Inspector für das Scannen von Azure-VMs verwenden möchten, müssen Sie die erforderlichen IAM-Rollen erstellen. Details hierzu finden Sie unter the section called “IAM-Rollen für das Scannen von VMs”.

9. Wenn Sie mit der Eingabe und Überprüfung der Einstellungen fertig sind, wählen Sie Connector erstellen.

IAM-Rollen für Azure-VM-Scans über Amazon Inspector

Um das Scannen von Sicherheitslücken über Amazon Inspector zu aktivieren, müssen Sie die folgenden IAM-Ressourcen in Ihrem AWS-Konto erstellen.

IAM OIDC-Identitätsanbieter

Erstellen Sie einen IAM-OIDC-Identitätsanbieter für mit der folgenden Konfiguration: Microsoft Entra ID

- URL des Ausstellers: `https://sts.windows.net/`*`tenant-id`*`/`
- Kunden-ID-Liste:`api://`*`app-id`*, `api://AzureADTokenExchange`

- Fingerabdruck: Eine 40-stellige Zeichenfolge, die ausschließlich Nullen enthält (40 Mal `0` wiederholt). AWS STS validiert Token über den JWKS-Endpunkt und nicht über den Fingerabdruckwert.

Inspector2VmScannerRole-*tenant-id*

Wird vom Amazon Inspector VM Scanner-Agent verwendet, der auf Azure-VMs ausgeführt wird, um Scan-Telemetrie an Amazon Inspector zu senden. Diese Rolle verwendet den OIDC-Web-Identitätsverbund über den Identitätsanbieter. Microsoft Entra ID

Vertrauensrichtlinie:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::account-id:oidc-provider/
sts.windows.net/tenant-id/"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "sts.windows.net/tenant-id/:aud": "api://app-id"
                }
            }
        }
    ]
}
```

Schlagworte:

- `inspector-managed` = `true`

Genehmigungsrichtlinie (TelemetryPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "inspector2-telemetry:*",
            "Resource": "*"
        }
    ]
}
```

Inspector2SSMFederationRole-*tenant-id*

Aktiviert den OIDC-Verbund mit Azure für eine sichere cloudübergreifende Authentifizierung. Diese Rolle wird von AssumeRole und und DispatchRole von Amazon EC2 Systems Manager übernommen, um Web-Identitätstoken für Azure-Operationen abzurufen.

Vertrauensrichtlinie:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/caller": "SSM"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
                        "arn:aws:iam::account-id:role/Inspector2SSMDispatchRole-tenant-
id"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
```

```
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Genehmigungsrichtlinie (FederationPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "sts:IdentityTokenAudience": [
                        "api://AzureADTokenExchange"
                    ]
                }
            },
            "Action": [
                "sts:GetWebIdentityToken",
                "sts:TagGetWebIdentityToken"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Schlagworte:

- `caller` = `SSM`
- `inspector-managed` = `true`

Inspector2SSMAssumeRole-*tenant-id*

Führt Amazon EC2 Systems Manager Automation aus, um Azure-VMs als verwaltete Instanzen zu integrieren. Diese Rolle erstellt und verwaltet Hybrid-Aktivierungen, übergibt Rollen an Amazon EC2 Systems Manager und ruft Automatisierungsdokumente ab.

Vertrauensrichtlinie:

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Genehmigungsrichtlinie (AssumeRolePolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/
AmazonEC2RunCommandRoleForManagedInstances",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateActivation",
```

```
                "ssm:DeleteActivation",
                "ssm:DescribeActivations",
                "ssm:DescribeInstanceInformation",
                "ssm:PutConfigurePackageResult",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:AddTagsToResource",
            "Resource": [
                "arn:aws:ssm:*:account-id:activation/*",
                "arn:aws:ssm:*:account-id:managed-instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetDocument",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:*:document/AWS-InstallSsmAgentOnAzure",
                "arn:aws:ssm:*::document/AmazonInspector2-InspectorVmScanner"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetCloudConnector",
            "Resource": "*"
        }
    ]
}
```

Schlagworte:

- `caller` = `SSM`
- `AzureTenantId` = *`tenant-id`*
- `AzureApplicationId` = *`app-id`*
- `inspector-managed` = `true`

Inspector2SSMDispatchRole-*tenant-id*

Löst Azure-VM-Ziele auf und leitet die Installation des Amazon Inspector VM Scanner-Agenten über Amazon EC2 Systems Manager Automation ein. Diese Rolle startet Automatisierungsausführungen und leitet AssumeRole sie an Amazon EC2 Systems Manager weiter.

Vertrauensrichtlinie:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Genehmigungsrichtlinie (DispatchPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:account-id:automation-execution/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:ListCloudConnectors",
                "ssm:GetCloudConnector",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Schlagworte:

- `caller` = `SSM`
- `inspector-managed` = `true`

Voraussetzungen für das Scannen virtueller Rechner

Bei der Azure-App-Registrierung muss der Anwendungs-ID-URI auf gesetzt sein`api://app-id`.

Für jede Azure-VM, die Sie scannen möchten, muss eine vom System zugewiesene verwaltete Identität aktiviert sein. Verwenden Sie eine DeployIfNotExists Richtlinie in Ihrer Azure-Umgebung, um neuen VMs automatisch verwaltete Identitäten zuzuweisen.

Nachdem Sie den Connector erstellt haben, beginnt Security Hub mit der Überwachung Ihrer Azure-Umgebung. Sie können den Status des Connectors auf der Seite Integrationen überprüfen.

Passen Sie den Umfang eines Azure-Connectors an

Nachdem Sie einen Microsoft Azure-Connector erstellt haben, können Sie den Umfang des Connectors anpassen, indem Sie die Azure-Abonnements oder Azure-Regionen ändern, die er überwacht. Bereichsänderungen werden bei Ressourcen mit Aktivitätsprotokollereignissen in der Regel innerhalb von 15 bis 30 Minuten wirksam. Die vollständige Evaluierung neu hinzugefügter Azure-Abonnements kann bis zu 24 Stunden dauern.

Bevor Sie den Umfang eines Connectors anpassen, sollten Sie Folgendes beachten:

- Wenn Sie den Geltungsbereich eines Connectors in Security Hub ändern, werden die zugehörigen serviceverknüpften Connectors in Security Hub CSPM und Amazon Inspector automatisch entsprechend aktualisiert.
- Der Umfang eines Security Hub-Connectors darf niemals geringer sein als der eines vorhandenen, vom Kunden verwalteten Connectors in Security Hub CSPM oder Amazon Inspector für denselben Azure-Mandanten.
- Wenn Sie dem Connector-Bereich eine Region hinzufügen, müssen Sie das Setup-Skript erneut ausführen, um die Event Hub-Infrastruktur in der neuen Region bereitzustellen. Ihre bestehende Event Hub-Konfiguration ist davon nicht betroffen.

Überprüfen Sie den Zustand eines Azure-Connectors

Sie können den Zustand eines Microsoft Azure-Connectors jederzeit überprüfen, um sicherzustellen, dass Security Hub Daten aus Ihrer Azure-Umgebung empfängt.

Um den Zustand eines Connectors zu überprüfen

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/advanced/home? region=us-ost-1. .
2. Wählen Sie im Navigationsbereich Integrationen und wählen Sie Ihren Azure-Connector aus.
3. Stellen Sie sicher, dass der Connector-Status Aktiv lautet. Wenn der Connector Aktiv anzeigt, ist die Überprüfung abgeschlossen. Wenn ein anderer Status angezeigt wird, finden Sie weitere Informationen unterthe section called “Problembehandlung bei einem Connector”.
4. Navigieren Sie zu Ergebnisse und filtern Sie `ResourceCloudProviders = Azure` nach, um sicherzustellen, dass Ergebnisse für Ihre Azure-Ressourcen generiert werden.
5. Überprüfen Sie auf der Seite mit den Sicherheitsstandards, ob der CIS Azure v4.0-Standard Kontrollen mit dem Status PASSED oder FAILED anzeigt (nicht alle NO_DATA).

> **Note**
>
> Der Integritätsstatus des Connectors ist letztendlich konsistent. Wenn ein Berechtigungs- oder Konfigurationsproblem auftritt, ändert sich der Status des Connectors schnell in Heruntergestuft und es wird eine umsetzbare Meldung angezeigt. Nachdem Sie das Problem behoben haben, kann es jedoch bis zu 24 Stunden dauern, bis der Status wieder zu Verbunden zurückkehrt.
>
> - Ein Status „Heruntergestuft“ nach einem kürzlich erfolgten Update weist nicht unbedingt auf ein anhaltendes Problem hin.
> - Überprüfen Sie die CloudWatch Metriken im Namespace, um in Echtzeit Einblick in die Fehler bei der Aufzeichnung zu erhalten.

Problembehandlung bei einem Azure-Connector

Wenn Sie Probleme mit Ihrem Connector haben, lesen Sie sich die folgenden häufigen Probleme und Lösungen durch.

Der Status des Connectors ist fehlerhaft

Dieses Problem tritt normalerweise auf, wenn Verbundanmeldeinformationen in Azure nicht korrekt konfiguriert sind.

Um dieses Problem zu beheben, stellen Sie sicher, dass die URL des Token-Ausstellers und der Betreff-ARN in Ihren Azure-Verbundanmeldedaten mit Ihren übereinstimmen. AWS-Konto

Keine Ergebnisse nach 30 Minuten

Dieses Problem kann auftreten, wenn der Event Hub keine Aktivitätsprotokolle empfängt.

Um dieses Problem zu beheben, überprüfen Sie, ob die Diagnoseeinstellungen in Ihren Azure-Abonnements konfiguriert sind und ob der Event Hub-Namespace korrekt mit `AWSConfig-`*`account-id`*`-`*`region`* gekennzeichnet ist.

Alle Steuerelemente zeigen NO_DATA

Dieses Problem kann auftreten, wenn der Connector deaktiviert ist oder wenn Sie Ihre AWS Config Azure-Umgebung nicht erreichen können.

Um dieses Problem zu beheben, stellen Sie sicher, dass der Connector aktiviert ist und dass der Dienstprinzipal im Bereich der Mandantenstammverwaltungsgruppe die Rolle Reader innehat.

Einige Azure-Ressourcen konnten nicht aufgezeichnet werden

Der Fehler kann aus einem der folgenden Gründe auftreten:

- Die Azure-Umgebung erfüllt nicht die Voraussetzungen für die Ressourcenaufzeichnung.
- Für die App-Registrierung ist keine Administrator-Zustimmung für Microsoft Graph-API-Berechtigungen erforderlich.
- Die Rollenzuweisung „Leser“ deckt nicht alle erforderlichen Bereiche ab.
- Der Microsoft Entra ID-Mandant verfügt nicht über die erforderlichen Protokolldaten.

Gehen Sie wie folgt vor, um den Fehler zu beheben:

1. Um zu überprüfen, ob Ihre Umgebung alle Anforderungen erfüllt, lesen Sie die Voraussetzungen für Microsoft Azure.
2. Vergewissern Sie sich mit Zustimmung des Administrators, dass die App-Registrierung über die erforderlichen Microsoft Graph-API-Berechtigungen verfügt.
3. Stellen Sie sicher, dass der Dienstprinzipal die Rolle Reader im Bereich der Stammverwaltungsgruppe des Mandanten innehat.

Die Ergebnisse werden nur für einige Abonnements angezeigt

Dieses Problem kann auftreten, wenn der Export des Aktivitätsprotokolls nicht für alle Zielabonnements konfiguriert ist.

Um dieses Problem zu beheben, stellen Sie sicher, dass die Diagnoseeinstellungen alle Abonnements abdecken, die im Connector-Bereich enthalten sind.

Wie Security Hub mit Ressourcen umgeht und Identifikatoren findet

Wenn Sie Ihre Azure-Integration für AWS Security Hub aktivieren, werden Ressourcen- und Sicherheitsfindungskennungen von anderen Cloud-Anbietern in AWS Config Security Hub und anderen AWS Diensten (je nach Bedarf) als Metadaten gespeichert, die sich auf die Verwaltung der entsprechenden Ressourcenkonfiguration und die von den anderen Cloud-Anbietern gesammelten Sicherheitsfindungsdaten beziehen. Solche Kennungen stellen nicht Ihre Inhalte dar. Nehmen Sie keine sensiblen, vertraulichen oder persönlich identifizierbaren Informationen in sie auf.

Die folgenden Identifikatoren aus Ihrer verbundenen Cloud-Umgebung werden gespeichert und verwendet, AWS um Multi-Cloud-Sicherheitsfunktionen bereitzustellen:

- Ressourcen-IDs: Azure-Mandanten-ID, Abonnement-ID, Standort (Region), Ressourcen-ID (Ressourcengruppen-IDs oder -namen, Ressourcenanbieter, Ressourcentyp)
- Identifikatoren für Sicherheitslücken: Die eindeutigen Kennungen, die jeder vom Erkennungsdienst generierten Sicherheitsfeststellung zugewiesen wurden.

Beziehungen zwischen diesen Identifikatoren — einschließlich der Beziehung zwischen Ressourcen und der Beziehung der Ergebnisse zu Ressourcen — werden ebenfalls als Service-Metadaten gespeichert. AWS verwendet diese Identifikatoren für die Korrelation von Ressourcen, für die Zuordnung von Ergebnissen zu Ressourcen, für die Protokollierung von Dienstabläufen und für die Deduplizierung.

Löschen eines Microsoft Azure-Connectors in Security Hub

Nachdem Sie einen Microsoft Azure-Connector in AWS Security Hub erstellt haben, können Sie ihn jederzeit löschen. Wenn Sie einen Connector löschen, beendet Security Hub die Durchführung von Statusmanagement-Checks und die Schwachstellenüberwachung für Ihre Azure-Umgebung. Security Hub generiert auch keine neuen Erkenntnisse und andere Daten über Ihre Umgebung. Ihre vorhandenen Ergebnisse werden 90 Tage lang aufbewahrt. Das Ressourceninventar bleibt unverändert, als der Connector gelöscht wurde, und wird nach 90 Tagen entfernt.

Wenn Sie einen Connector löschen, löscht Security Hub automatisch die zugehörigen serviceverknüpften Connectors in AWS Security Hub CSPM und Amazon Inspector. Security Hub löscht die Azure-Anwendungsregistrierung und die Event Hub-Infrastruktur in Ihrer Azure-Umgebung nicht. Sie müssen diese manuell direkt in Microsoft Azure löschen. Informationen zur Vorgehensweise finden Sie unter Entfernen einer Anwendung in der Microsoft Azure-Dokumentation.

So löschen Sie einen Azure-Connector

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie den Connector aus, den Sie löschen möchten.
4. Wählen Sie Löschen aus.
5. Bestätigen Sie, dass Sie den Connector löschen möchten, wenn Sie dazu aufgefordert werden.

> **Important**
>
> Wenn Sie einen Connector löschen und innerhalb von 6 Stunden einen neuen erstellen, kann die Ressourcenerkennung bis zu 6 Stunden dauern. Planen Sie das Löschen und die Neuerstellung des Connectors entsprechend ein.

Arbeiten im Übersichts-Dashboard in Security Hub

Das Übersichts-Dashboard in der Security Hub-Konsole bietet einen Überblick über Ihre Risiken, Bedrohungen, Ressourcen und die Sicherheitsabdeckung aller Sicherheits-Widgets. Sie können das Dashboard anpassen, indem Sie Widgets hinzufügen und entfernen und indem Sie Filtersätze erstellen und anwenden, um Daten in jedem Widget abzurufen.

Überlegungen

Beachten Sie Folgendes, bevor Sie mit dem Dashboard interagieren:

- Anpassungen wie gespeicherte Filtersätze oder Änderungen am Layout von Widgets werden automatisch gespeichert.
- Die Daten werden jedes Mal automatisch aktualisiert, wenn Sie das Dashboard öffnen.
- Wenn Sie die regionsübergreifende Aggregation konfigurieren, enthält das Dashboard Ergebnisse aus all Ihren verknüpften Regionen (wenn Sie das Dashboard in Ihrer Heimatregion aufrufen).

Beachten Sie Folgendes, wenn es sich bei Ihrem Konto um ein delegiertes Administratorkonto für eine Organisation, ein Mitgliedskonto in einer Organisation oder ein eigenständiges Konto handelt.

- Anpassungen, die von einem delegierten Administratorkonto vorgenommen wurden, werden unabhängig von Anpassungen gespeichert, die von Mitgliedskonten vorgenommen wurden. Zu den Anpassungen können gespeicherte Filtersätze oder Änderungen am Layout von Widgets gehören.
- Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto für eine Organisation handelt, umfassen die Daten Ergebnisse für Ihr Konto und Ihre Mitgliedskonten.
- Wenn es sich bei Ihrem Konto um ein Mitgliedskonto in einer Organisation oder um ein eigenständiges Konto handelt, enthalten die Daten nur Ergebnisse für Ihr Konto.

Es hat sich bewährt, keine vertraulichen, sensiblen oder persönlich identifizierbaren Informationen (PII) in gespeicherte Filtersätze, benutzerdefinierte Widgets oder andere zugehörige Freiform-Textfelder aufzunehmen.

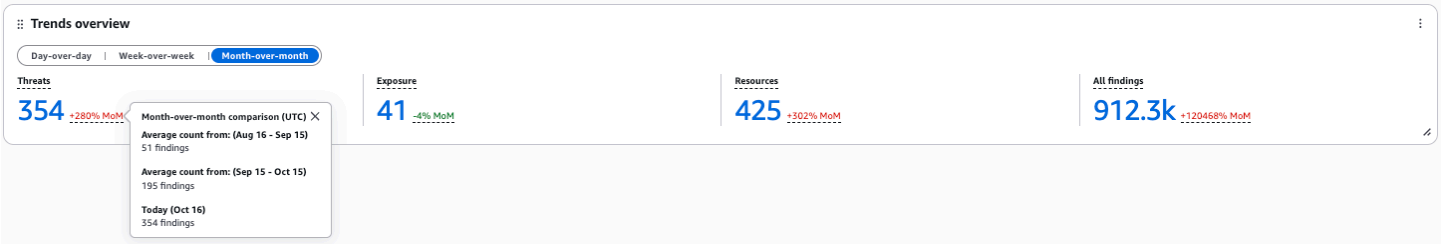
Verfügbare Widgets

Auf den Tabs „Geschäftsleitung“ und „Triage“ des Übersichts-Dashboards können Sie mit verschiedenen Widgets interagieren. Der Tab „Geschäftsleitung“ enthält Widgets, die Trenddaten zu Ihren Risiken, Bedrohungen und Ressourcen anzeigen, und das Widget „Sicherheitsabdeckung“, mit dem Sie die Deckung Ihres Kontos anhand der verschiedenen Sicherheitsfunktionen verfolgen können. Der Tab „Triage“ enthält Widgets, die eine Zusammenfassung Ihrer Risiken, Bedrohungen und Ressourcen anzeigen. Sie können jedoch Widgets hinzufügen, Widgets entfernen und die Position der einzelnen Widgets in beiden Tabs verwalten, um Ihr Erlebnis individuell zu gestalten.

Widgets für Trends

Die folgenden Widgets zeigen Trenddaten zu Ihren Risiken, Bedrohungen und Ressourcen an, sodass Sie sie im Laufe der Zeit analysieren können.

Widget „Übersicht über Trends“



Dieses Widget zeigt einen Überblick über Ihre Risiken, Bedrohungen, Ressourcen und Ergebnisse in den folgenden Zeiträumen:

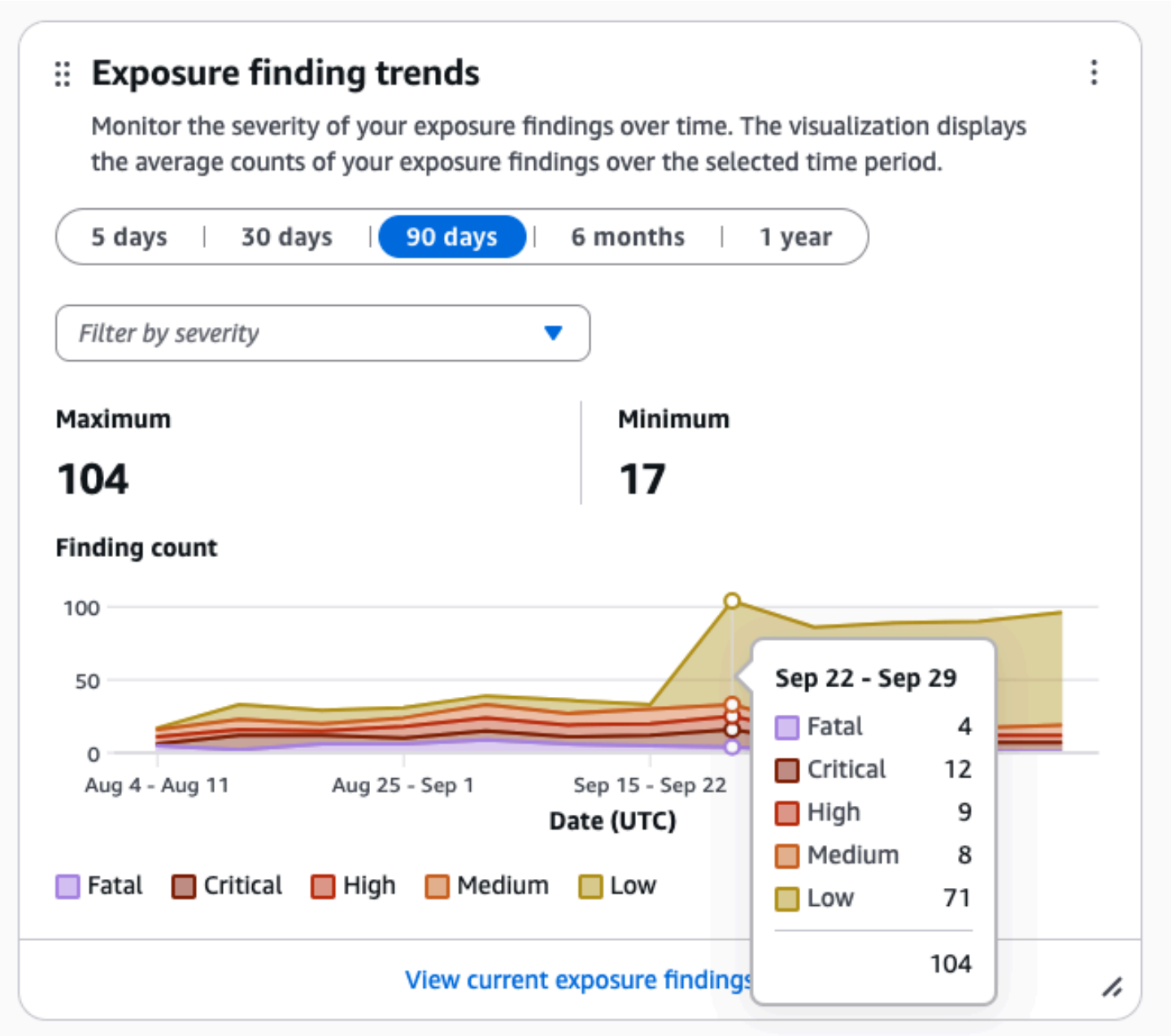
- Month-over-monthgibt die Anzahl der letzten zwei Monate im Vergleich zum Berichtszeitraum wieder.
- Week-over-weekgibt die Anzahl der letzten zwei Wochen im Vergleich zum Zeitraum wieder.
- Day-over-daygibt die Anzahl der letzten 2 Tage für den Zeitraum im Vergleich zum Zeitraum an.

Die Zahl neben dem Prozentsatz gibt den bisherigen Durchschnittswert für den gesamten Zeitraum wieder. Wenn Sie diese Zahl wählen, werden Sie zum entsprechenden Dashboard in der Konsole weitergeleitet. Wenn Sie zu einem anderen Dashboard navigieren, das Trenddaten anzeigt, zeigt das

Dashboard nur Trenddaten der letzten 90 Tage an oder in einem Zeitraum, der am besten geeignet ist, wenn Ihr Konto keine Ergebnisse oder Ressourcen enthält, die älter als 30 Tage sind.

> **Note**
>
> Um Daten in diesem Widget zu empfangen, müssen Sie die folgenden Sicherheitsdienste aktivieren:
>
> - AWS Security Hub CSPM — Um Daten über Gefahren zu erhalten
> - Amazon Inspector — Um Daten über Risiken zu erhalten
> - GuardDuty— Um Daten über Bedrohungen zu erhalten

Widget zur Ermittlung von Trends bei der Gefährdung



Dieses Widget zeigt den Schweregrad Ihrer Expositionsergebnisse in den folgenden Zeiträumen an:

- 5 Tage
- 30 Tage
- 90 Tage
- 6 Monate
- 1 Jahr

Die Visualisierung zeigt die durchschnittliche Anzahl Ihrer Ergebnisse im ausgewählten Zeitraum an.

Filter für Schweregrad

Sie können das Diagramm aktualisieren, indem Sie die folgenden Schweregradfilter ein- oder ausschließen:

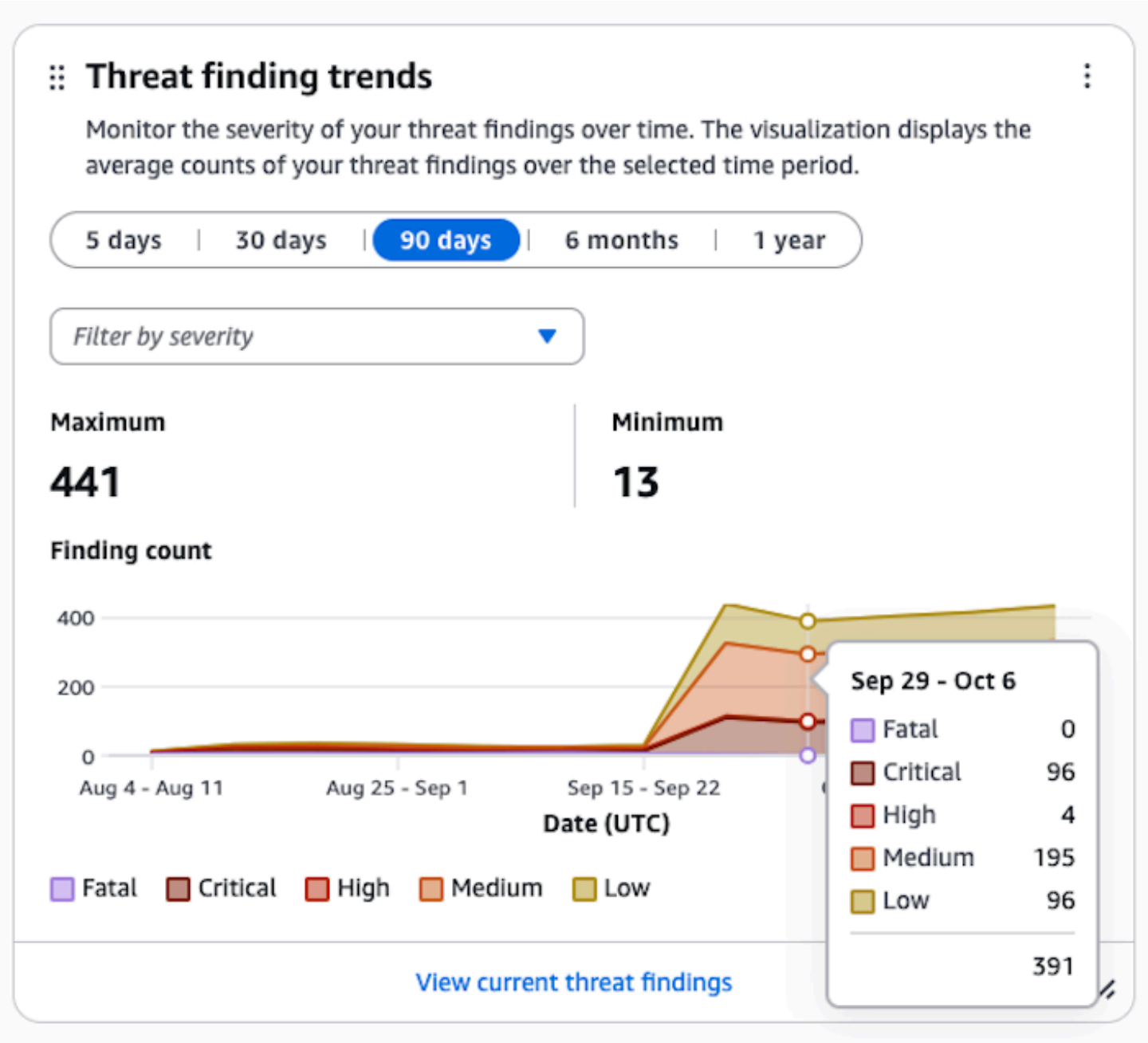
- Tödlich
- Critical
- Hoch
- Mittel
- Niedrig
- Informativ
- Sonstige
- Unbekannt

Angewendete Schweregradfilter werden am unteren Rand der Visualisierung in verschiedenen Feldern angezeigt. Sie können den Mauszeiger über die Visualisierung bewegen, um die durchschnittliche Anzahl der Ergebnisse für bestimmte Zeitpunkte zu überprüfen. Sie können auch die durchschnittliche Anzahl der Ergebnisse überprüfen, die jedem angewendeten Schweregradfilter entsprechen.

Sie können „Alle aktuellen Expositionsergebnisse anzeigen“ wählen, um zum Expositions-Dashboard weitergeleitet zu werden. Standardmäßig zeigt das Expositions-Dashboard nur Trenddaten der letzten 90 Tage an. Wenn Ihr Konto keine Expositionsergebnisse enthält, die älter als 30 Tage sind, zeigt das Dashboard Trenddaten an, die auf einem Zeitraum basieren, der am besten geeignet ist.

> **Note**
>
> Um Daten in diesem Widget zu empfangen, müssen Sie Amazon Inspector und Security Hub CSPM aktivieren.

Widget zur Erkennung von Bedrohungen: Trends



Dieses Widget zeigt den Schweregrad Ihrer Bedrohungsergebnisse in den folgenden Zeiträumen an:

- 5 Tage
- 30 Tage
- 90 Tage
- 6 Monate
- 1 Jahr

Die Visualisierung zeigt die durchschnittliche Anzahl Ihrer Ergebnisse im ausgewählten Zeitraum an.

Filter für Schweregrad

Sie können das Diagramm aktualisieren, indem Sie die folgenden Schweregradfilter ein- oder ausschließen:

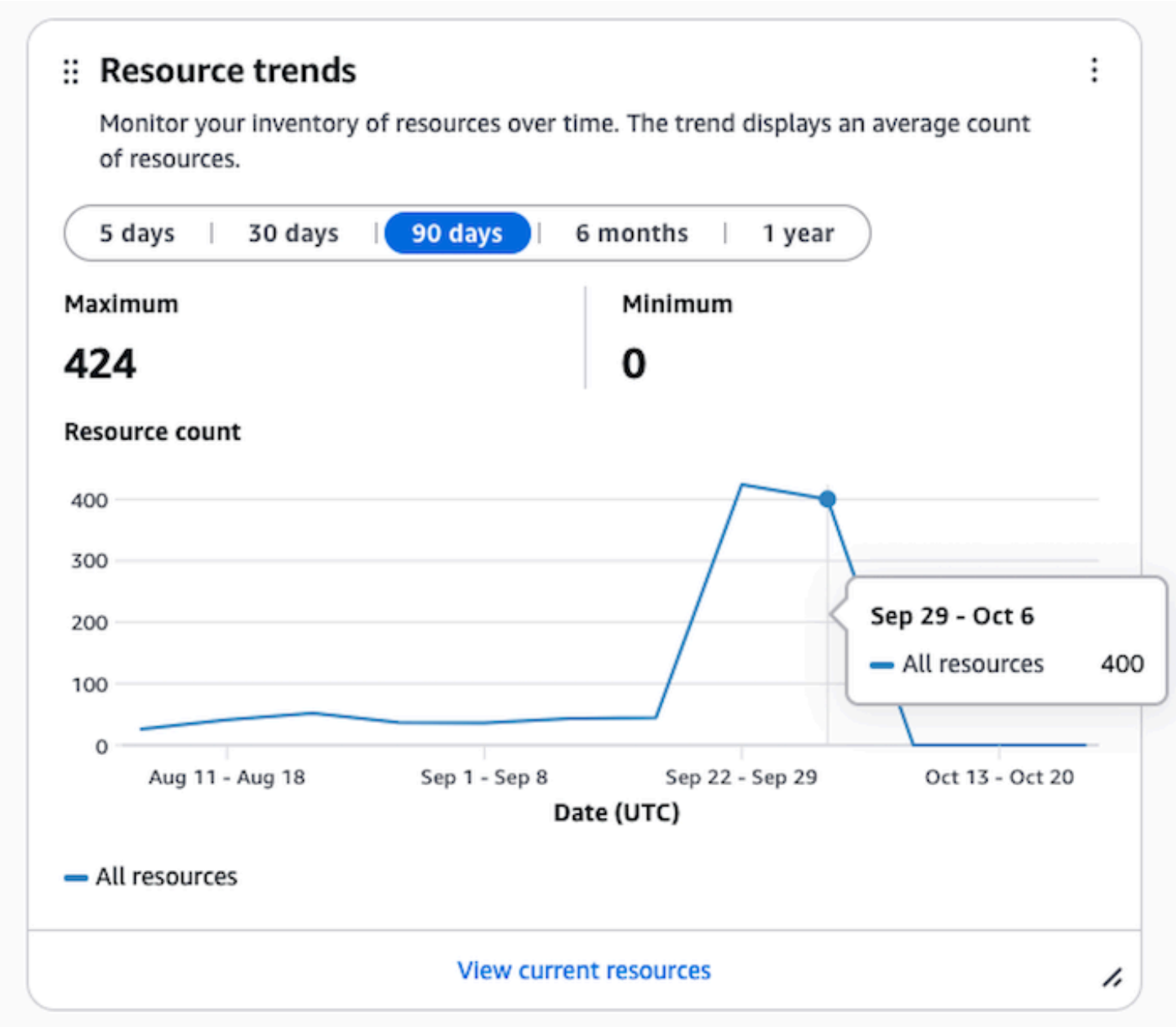
- Tödlich
- Critical
- Hoch
- Mittel
- Niedrig
- Informativ
- Sonstige
- Unbekannt

Angewendete Schweregradfilter werden am unteren Rand der Visualisierung in verschiedenen Feldern angezeigt. Sie können den Mauszeiger über die Visualisierung bewegen, um die durchschnittliche Anzahl der Ergebnisse für bestimmte Zeitpunkte zu überprüfen. Sie können auch die durchschnittliche Anzahl der Ergebnisse überprüfen, die jedem angewendeten Schweregradfilter entsprechen.

Sie können „Alle aktuellen Bedrohungsergebnisse anzeigen“ wählen, um zum Expose-Dashboard weitergeleitet zu werden. Standardmäßig zeigt das Bedrohungs-Dashboard nur Trenddaten der letzten 90 Tage an. Wenn Ihr Konto keine Bedrohungsergebnisse enthält, die älter als 30 Tage sind, zeigt das Dashboard Trenddaten an, die auf einem Zeitraum basieren, der am besten geeignet ist.

> **Note**
>
> Um Daten in diesem Widget zu empfangen, müssen Sie es aktivieren GuardDuty.

Widget „Ressourcentrends“



Dieses Widget zeigt eine Bestandsaufnahme Ihrer Ressourcen in den folgenden Zeiträumen an:

- 5 Tage
- 30 Tage
- 90 Tage
- 6 Monate
- 1 Jahr

Die Visualisierung zeigt die durchschnittliche Anzahl Ihrer Ressourcen im ausgewählten Zeitraum an. Sie können den Mauszeiger über die Visualisierung bewegen, um die durchschnittliche Anzahl der Ressourcen für bestimmte Zeitpunkte zu überprüfen.

Sie können Aktuelle Ressourcen anzeigen wählen, um zum Ressourcen-Dashboard weitergeleitet zu werden. Standardmäßig zeigt das Ressourcen-Dashboard nur Trenddaten der letzten 90 Tage an. Wenn Ihr Konto keine Ressourcen enthält, die älter als 30 Tage sind, zeigt das Dashboard Trenddaten an, die auf einem Zeitraum basieren, der am besten geeignet ist.

Dieses Widget zeigt eine Bestandsaufnahme Ihrer Ressourcen in den folgenden Zeiträumen an:

- 5 Tage
- 30 Tage
- 90 Tage
- 6 Monate
- 1 Jahr

Aufbewahrung von Daten für Trends

Security Hub speichert Trenddaten ein Jahr lang für alle AWS-Konten , für die Security Hub aktiviert ist. Nachdem Trenddaten ein Jahr lang aufbewahrt wurden, werden sie aus Security Hub gelöscht.

Trenddaten für delegierte Administrator- und eigenständige Konten werden gelöscht, nachdem Security Hub deaktiviert oder wenn die Konten gekündigt werden.

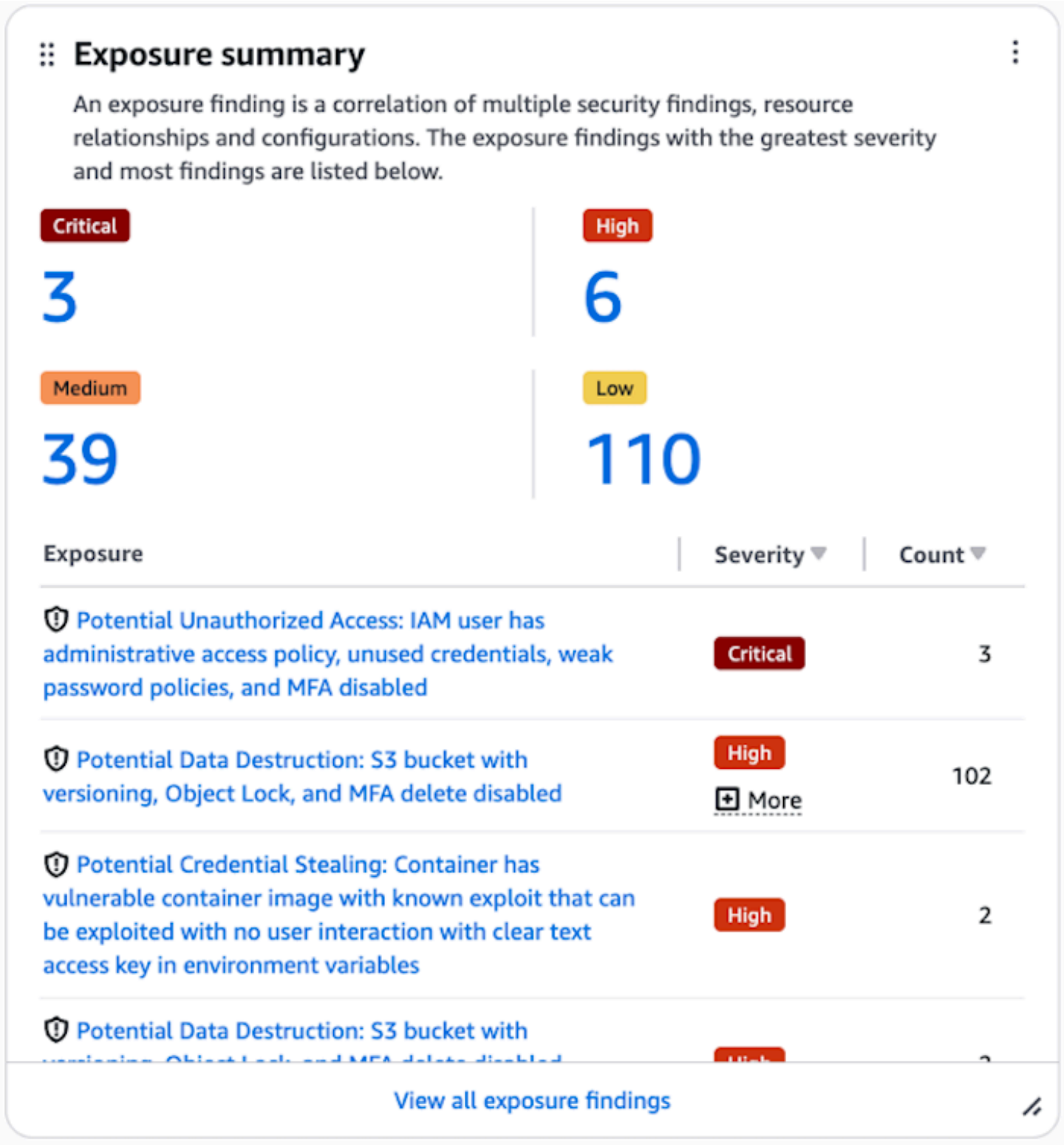
Trendszenarien zur Datenspeicherung für Mitgliedskonten mit aktiviertem Security Hub:

- Wenn ein Mitgliedskonto seine Organisation verlässt, speichert Security Hub die Trenddaten weiterhin ein Jahr lang, bis das Konto das Unternehmen verlassen hat.
- Wenn Security Hub für ein Mitgliedskonto deaktiviert ist, speichert Security Hub die Trenddaten ein Jahr lang, bis das Konto deaktiviert wurde.
- Wenn ein Mitgliedskonto gekündigt wird, trennt Security Hub die Trenddaten vom gekündigten Konto (z. B. indem die gekündigte Konto-ID gelöscht wird) und speichert die restlichen Trenddaten ein Jahr lang.

Übersichts-Widgets

Die folgenden Widgets zeigen eine Zusammenfassung Ihrer Risiken, Bedrohungen und Ressourcen an.

Widget „Risikoübersicht“

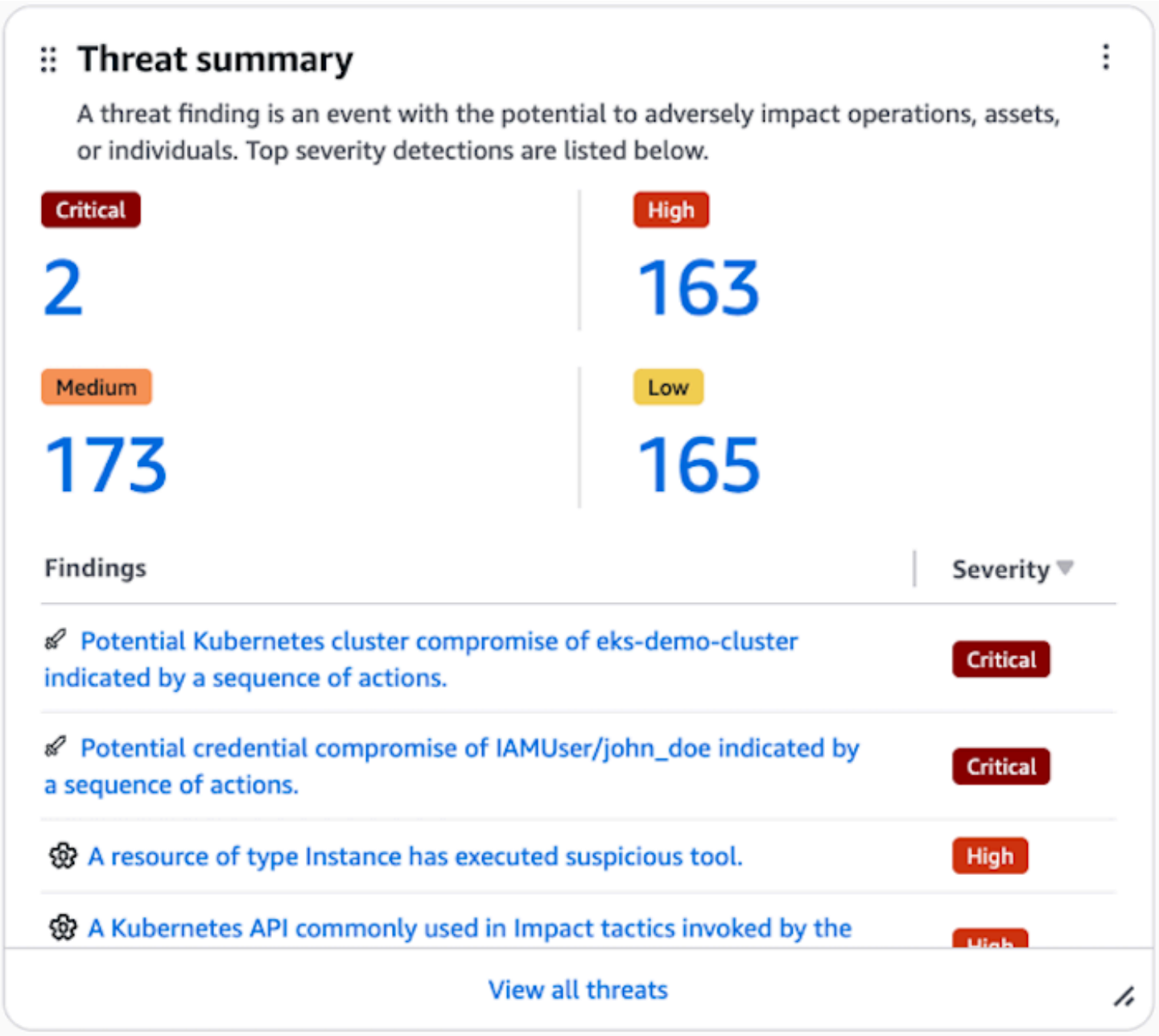


Dieses Widget zeigt Ihre Risiken nach Schweregrad an. Ein Risiko basiert auf einer Analyse der Ergebnisse und Merkmale von Security Hub und anderen AWS Sicherheitsdiensten wie Amazon

Inspector. Die Liste der Risiken in diesem Widget ist auf die acht Risiken mit dem höchsten Schweregrad beschränkt. Expositionen mit höherem Schweregrad werden in der Liste an erster Stelle angezeigt. Wenn zwei oder mehr Expositionen den gleichen Schweregrad haben, gruppiert die Liste diese Expositionen automatisch hinter den neueren Expositionen. Wenn Sie „Alle Expositionen anzeigen“ wählen, werden Sie zum Expositions-Dashboard weitergeleitet.

> **Note**
>
> Um Daten in diesem Widget zu empfangen, müssen Sie Amazon Inspector und Security Hub CSPM aktivieren.

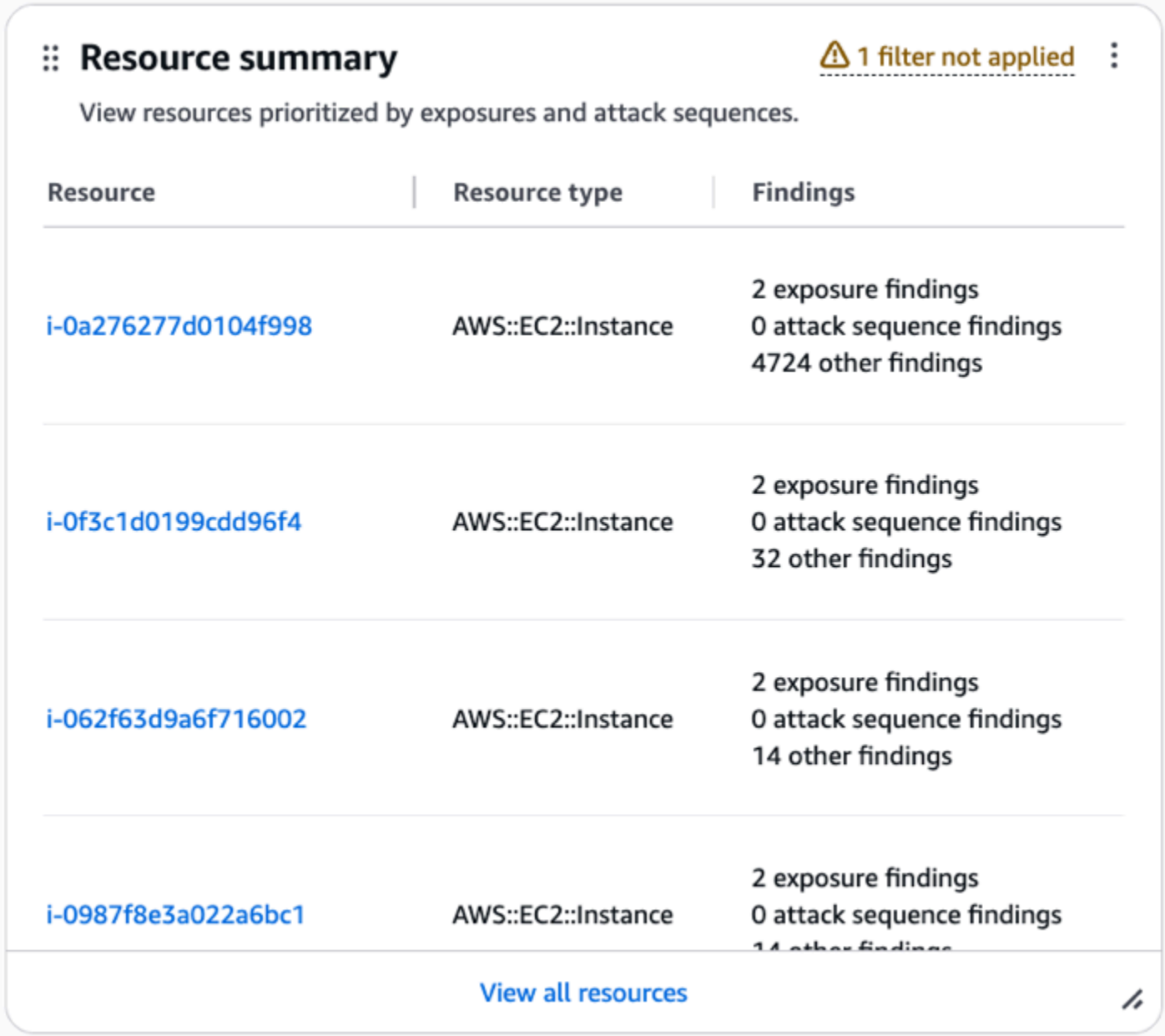
Widget „Zusammenfassung der Bedrohung“



Dieses Widget zeigt Ihre Bedrohungen nach Schweregrad an. Eine Bedrohung bezieht sich auf bösartige oder verdächtige Aktivitäten, die die Sicherheit Ihrer Umgebung gefährden können. Die Liste der Bedrohungen in diesem Widget ist auf die acht Bedrohungen mit dem höchsten Schweregrad beschränkt. Bedrohungen mit höherem Schweregrad werden in der Liste an erster Stelle angezeigt. Wenn zwei oder mehr Bedrohungen den gleichen Schweregrad haben, gruppiert die Liste diese Bedrohungen automatisch hinter neueren Bedrohungen. Wenn Sie Alle Bedrohungen anzeigen wählen, werden Sie zum Bedrohungs-Dashboard weitergeleitet.

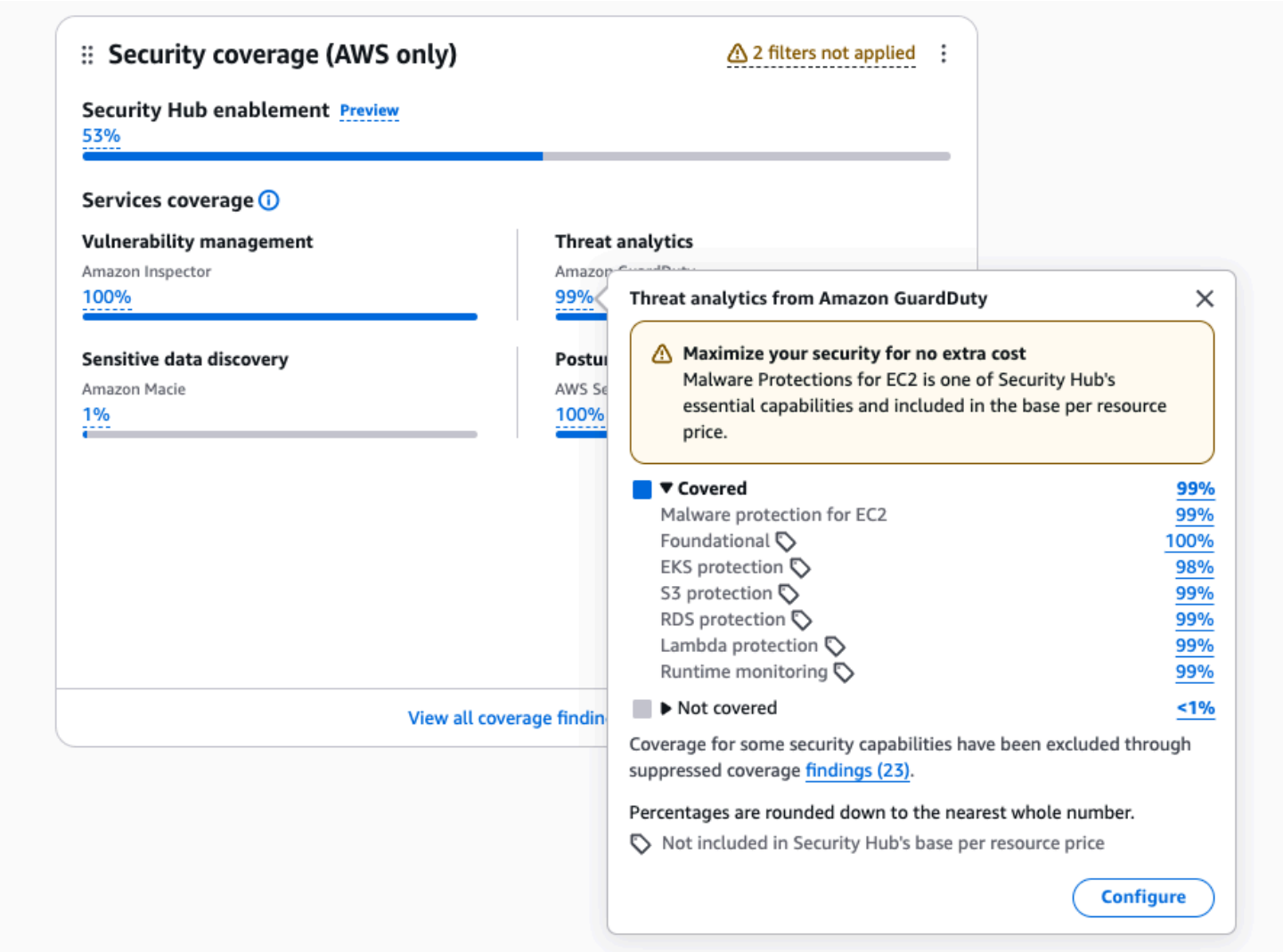
> **Note**
>
> Um Daten in diesem Widget zu empfangen, müssen Sie es aktivieren GuardDuty.

Widget „Zusammenfassung der Ressourcen“



Dieses Widget zeigt Ressourcen nach Typ und den Ressourcen zugeordnete Ergebnisse an. Ressourcen werden nach Risiken und Angriffssequenzen priorisiert. Wenn Sie Alle Ressourcen anzeigen wählen, werden Sie zum Ressourcen-Dashboard weitergeleitet.

Widget „Sicherheitsabdeckung“



Das Widget zeigt eine Zusammenfassung der Deckung Ihres Kontos für die folgenden Sicherheitsfunktionen an:

- Schwachstellenmanagement durch Amazon Inspector
- Erkennung von Bedrohungen durch Amazon GuardDuty
- Entdeckung sensibler Daten durch Amazon Macie
- Bestandsverwaltung durch AWS Security Hub CSPM

Bei delegierten Administratorkonten zeigt das Widget auch die Kontoabdeckung für die Aktivierung von Security Hub an.

Für jedes Deckungselement wird ein Prozentsatz angezeigt, der der Aktivierung dieser Funktion in Ihren Konten entspricht. Wenn Sie einen Prozentsatz auswählen, werden Details zur Deckung für diese Funktion angezeigt. Wenn Sie den Prozentsatz der Security Hub-Aktivierung auswählen, wird ein Seitenbereich angezeigt. Das Feld zeigt, wie viele Konten in jeder Region Ihres Unternehmens aktiviert sind.

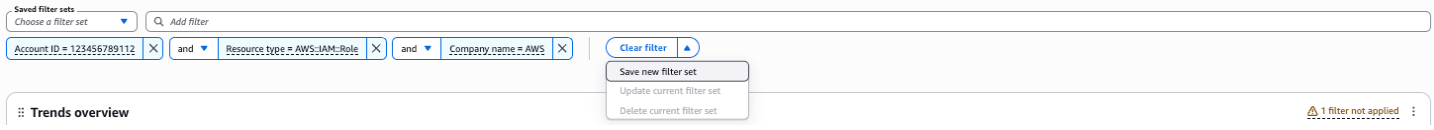
Im Abschnitt Serviceumfang geben Prozentsätze den Anteil der Abdeckungsprüfungen an, die für jede Sicherheitsfunktion bestanden wurden. Diese Prüfungen beziehen sich auf die Konten und Regionen, in denen Security Hub aktiviert ist. Wenn Sie einen Prozentsatz der Deckung auswählen, wird ein Popover angezeigt, in dem jede Funktion als Abgedeckt (Prüfung bestanden) oder Nicht abgedeckt (Prüfung nicht bestanden) aufgeschlüsselt wird. Prozentsätze werden auf die nächste ganze Zahl abgerundet. Wenn Sie im Popover einen beliebigen Prozentsatz auswählen, wird die Seite mit den Ergebnissen der Berichterstattung mit Details zu den Ergebnissen geöffnet, aus denen sich dieser Prozentsatz zusammensetzt. Wählen Sie Konfigurieren, um den einzelnen Dienst zu öffnen, in dem Sie die Konfiguration für diese Funktion verwalten können, oder um die Security Hub-Konfigurationsseite zu öffnen, auf der Sie Ihre Konfigurationen für Sicherheitsdienste aktualisieren können.

Wenn einer Ihrer Schutzbefunde in Security Hub unterdrückt wird, zeigt das Widget eine Meldung an, die Sie darüber informiert, dass der Schutz ausgeschlossen wurde: Der Schutz für Sicherheitsfunktionen wurde aufgrund unterdrückter Abdeckungsergebnisse ausgeschlossen.

Weitere Informationen zum Anzeigen und Unterdrücken von Deckungsergebnissen finden Sie unter Abdeckungsergebnisse in Security Hub.

Verfügbare Filter

Mithilfe der Leiste „Filter hinzufügen“ können Sie Filter auf Sicherheits-Widgets anwenden.



Filter sind in die folgenden Kategorien unterteilt:

- Geteilte Filter — gilt für alle Sicherheits-Widgets
- Suchfilter — gilt für Sicherheits-Widgets, die Suchdaten anzeigen
- Ressourcenfilter — gilt für Sicherheits-Widgets, die Ressourcendaten anzeigen

Sie können einen Filtersatz erstellen, indem Sie Filter mithilfe der Operatoren und/oder verbinden und dann in der Dropdownliste die Option Neuen Filtersatz speichern auswählen.

Filter, die auf das Widget „Trends bei der Suche nach Bedrohungen“ und das Widget „Trends bei der Suche nach Bedrohungen“ angewendet werden

Derzeit werden für diese Widgets unter anderem die folgenden Filter unterstützt:

- Konto-ID
- Klassennamen finden
- Ergebnistyp
- Product Name (Produktname)
- Region
- Status

Filter, die auf das Widget „Ressourcentrends“ angewendet werden

Derzeit werden für dieses Widget unter anderem die folgenden Filter unterstützt:

- Konto-ID
- Region
- Kategorie „Ressource“
- Ressourcentyp

Filter werden nicht auf Widgets angewendet



Wenn ein Widget keinen Filter unterstützt, wird der Filter nicht auf das Widget angewendet. In diesem Fall zeigt das Widget eine Warnmeldung an, die Sie darüber informiert, wie viele Filter nicht angewendet wurden, und listet die Namen der Filter auf, die es nicht unterstützt.

Details zu Ressourcen in Security Hub anzeigen

Auf der Seite Ressourcen werden häufig verwendete Ressourcen in Ihrem Konto und Ihrer Organisation nachverfolgt. Sie können auf die Ressourcenseite in der Security Hub-Konsole zugreifen, indem Sie im Navigationsbereich Ressourcen auswählen. Der Vorteil der Seite Ressourcen besteht darin, dass sie Ihnen hilft, Ihr Sicherheitsniveau zu überwachen, Ihre Ressourcen zu organisieren und Details zu Ihren Ressourcen zu überprüfen. Wenn Sie einen Ressourcentyp auswählen, können Sie alle Ressourcen überprüfen, die dem Ressourcentyp zugeordnet sind. Sie können alle Ergebnisse überprüfen, die mit einer Ressource verknüpft sind. Zu den auf der Seite Ressourcen verfügbaren Ressourcentypen gehören alle Ressourcen in Ihren Konten, für die AWS Sicherheitsdienste zuständig sind, die Ergebnisse zu Security Hub beitragen.

> **Note**
>
> Der delegierte Administrator kann alle Ressourcen einsehen, die Mitgliedskonten zugeordnet sind. Wenn Sie ein Zuhause konfiguriert haben AWS-Region, können Sie alle Ihre Ressourcen in AWS-Region Ihrem Zuhause über Links AWS-Regionen einsehen.

Wenn Sie eine Ressource auswählen, können Sie die Details zu dieser Ressource überprüfen. Zu diesen Details gehören der Name, die ID, der ARN, der Typ und die Kategorie der Ressource. Sie können die mit der Ressource verknüpfte Konto-ID überprüfen, wann die Ressource erstellt wurde (Zeitstempel) und wo die Ressource erstellt wurde (AWS-Region). Sie können auch zusätzliche Konfigurationsdetails zur Ressource überprüfen. Diese Details finden Sie in einem JSON-Snippet, das Sie kopieren können.

Wenn Sie von der Registerkarte „Übersicht“ zur Registerkarte „Ergebnisse“ wechseln, können Sie alle Ergebnisse überprüfen, die mit der Ressource verknüpft sind. Auf der Registerkarte Ergebnisse werden der Name jedes Befundes, die Art jedes Befundes und der Schweregrad jedes Befundes angezeigt. Sie können Ergebnisse nach verschiedenen Feldern gruppieren und mithilfe von Filtern nach Ergebnissen suchen. Wenn Sie ein Ergebnis auswählen, können Sie sich einen Überblick über das Ergebnis verschaffen, der Informationen zur Einhaltung der Vorschriften und zur Behebung von Problemen im Zusammenhang mit dem Ergebnis enthält. Auf der Registerkarte „Eigenschaften“ werden alle Merkmale angezeigt, die für die Ressource identifiziert wurden. Du kannst dir die Eigenschaften ansehen, die dazu beigetragen haben, einen Risikopositionsergebnis für die Ressource zu erstellen. Sie können auch kontextuelle Merkmale sehen, bei denen es sich um andere Sicherheitselemente handelt, die für die Ressource identifiziert wurden, aber nicht direkt zu den Risikopositionsergebnissen beigetragen haben. Wenn Sie zur Ressource zurückkehren, können

Sie Ressource öffnen wählen, um die Ressource in der Konsole auf ihren Ressourcentyp hin zu überprüfen. Wenn es sich bei der Ressource beispielsweise um eine IAM-Ressource handelt, können Sie die Ressource in der IAM-Konsole öffnen.

Die Ressourcenseite bietet Ihnen verschiedene Möglichkeiten, Ressourcen zu organisieren und nach ihnen zu suchen. Sie können Ressourcen nach Typ gruppieren. Beispielsweise können Sie Ressourcen nach Konto-ID, Suchtyp, Ressourcenkategorie AWS-Region, Ressourcenname und Ressourcentyp gruppieren. Mithilfe von Schnellfiltern können Sie Ressourcen nach Kategorie, Konten und Suchtypen überprüfen.

Security Hub und das Open Cybersecurity Schema Framework (OCSF)

Security Hub verwendet das Open Cybersecurity Schema Framework (OCSF) als Standardformat für alle Sicherheitsergebnisse. In diesem Thema wird OCSF beschrieben und wie Security Hub es implementiert.

OCSF im Überblick

Die Ergebnisse von Security Hub werden mithilfe von OCSF (Open Cybersecurity Schema Framework) formatiert. OCSF ist ein Open-Source-Projekt, das ein erweiterbares Framework für die Entwicklung von Schemas sowie ein herstellerunabhängiges Kernsicherheitsschema bereitstellt. Anbieter und andere Datenproduzenten können das Schema für ihre spezifischen Domänen übernehmen und erweitern. Datenproduzenten können unterschiedliche Schemas abbilden, um Sicherheitsteams dabei zu helfen, die Datenaufnahme und -normalisierung zu vereinfachen, sodass Datenwissenschaftler und Analysten bei der Erkennung und Untersuchung von Bedrohungen mit einer gemeinsamen Sprache arbeiten können. Ziel ist es, einen offenen Standard bereitzustellen, der in jeder Umgebung, Anwendung oder Lösung Anwendung findet und gleichzeitig bestehende Sicherheitsstandards und -prozesse ergänzt.

Das Framework besteht aus Datentypen, einem Attributwörterbuch und einer Taxonomie. Obwohl es nicht auf Cybersicherheit oder Ereignisse beschränkt ist, liegt der anfängliche Schwerpunkt auf Cybersicherheitsereignisschemas. OCSF ist unabhängig von Speicherformat, Datenerfassungsmethoden und ETL-Prozessen.

Security Hub unterstützt derzeit die Ergebnisse der OCSF-Schemaversion 1.6.

Zugehörige Ressourcen

Weitere Informationen zu OCSF und seiner Implementierung finden Sie in den folgenden Ressourcen:

- Öffentliche OCSF-Dokumentation
- Dokumentation zur Verwendung der OCSF-Erweiterung
- Referenz zum OCSF-Kernschema
- OCSF-Erweiterungsregistrierung

AWS Erweiterung für OCSF

OCSF-Schemas können durch Hinzufügen neuer Attribute, Objekte, Kategorien, Profile und Ereignisklassen erweitert werden. Ein Schema ist die Aggregation von Kernschemaentitäten und Erweiterungen.

OCSF-Erweiterungen ermöglichen es einem bestimmten Anbieter oder Kunden, ein vorhandenes Schema durch Hinzufügen von Attributen zu erweitern, um domänenspezifische Anpassungen zu ermöglichen, die Dateninteroperabilität zu verbessern und detaillierteren Kontext für Sicherheitsanalysen hinzuzufügen.

Die AWS Erweiterung für das Open Cybersecurity Schema Framework (OCSF) bietet Attributdefinitionen für Cloud-Ressourcen innerhalb von OCSF-Ereignissen. Diese Erweiterung fügt ein `cloud_resources` Profil hinzu, das das `resource_details` OCSF-Objekt um cloudspezifische Ressourcenattribute erweitert. Mit diesen Attributen können Sicherheitsteams Ressourcenkonfigurationen, potenzielle Sicherheitslücken und Metadaten zur Bedrohungserkennung analysieren.

Erweitertes **`resource_details-Objekt`**

Die AWS Erweiterung erweitert das `resource_details` Objekt um Attribute, die in der Liste der Attributreferenzen unten aufgeführt sind. Diese Attribute gewährleisten die korrekte Identifizierung und Klassifizierung von Cloud-Ressourcen verschiedener Anbieter innerhalb standardisierter Event-Frameworks.

AWS Erweiterung für die OCSF-Attributreferenz

Die Abschnitte Basisattribute und Ressourcenspezifische Objekte enthalten Beispiele für jedes der Attribute, die Teil der AWS OCSF-Erweiterung für resource_details sind.

Jede der Attributdefinitionen enthält einen OCSF-Status, der ihre aktuelle Beziehung zum öffentlichen OCSF-Schema beschreibt:

- Bestehend: Dieses Attribut war bereits in der Standard-OCSF-Ressource resource_details enthalten und ist jetzt Teil der Erweiterung. AWS
- Neu: Das Attribut ist nicht Teil von OCSF und wurde als Teil der Erweiterung eingeführt. AWS Es ist im OCSF-Kernschema nicht vorhanden.
- Zu resource_details hinzugefügt: Das Attribut ist in OCSF definiert, aber nicht Teil von resource_details.

Grundlegende Attribute

Dies sind grundlegende Attribute, die für die Identifizierung von Ressourcen, den Standort und grundlegende Metadaten verwendet werden. Sie bestehen aus einfachen Datentypen wie Zeichenketten, Zeitstempeln und Arrays.

Cloud-Partition

Die Cloud-Partition, in der die Ressource vorhanden ist.

Anforderung

Empfohlen

Typ

Zeichenfolge

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "cloud_partition": "aws"
    }
  ]
```

```
}
```

Konto-ID des Besitzers

Eine 12-stellige Kontokennung, zu der die Ressource gehört.

Anforderung

Empfohlen

Typ

Zeichenfolge

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      }
    }
  ]
}
```

Ressourcentyp

Der AWS CloudFormation Ressourcentyp, der den spezifischen Dienst und die Ressource identifiziert.

Anforderung

Erforderlich

Typ

Zeichenfolge

Format

Muss der Benennungskonvention für AWS CloudFormation Ressourcentypen folgen: `AWS::<Service>::<ResourceType>`

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "type": "AWS::EC2::Instance"
    }
  ]
}
```

Ressourcen-ID

Die eindeutige Kennung für die Cloud-Ressource (z. B. i-1234567890abcdef0).

Anforderung

Empfohlen

Typ

Zeichenfolge

Format

Muss eine gültige Ressourcen-ID sein. Mindestlänge 1. Die maximale Länge beträgt 768.

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
```

```
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

Alternative Ressourcenkennung

Die eindeutige Kennung für die Cloud-Ressource, in der Regel der Amazon-Ressourcenname (ARN).

Anforderung

Empfohlen

Typ

Zeichenfolge

Format

Sollte ein gültiger AWS ARN sein. Zu den gängigen Mustern gehören:

- `"arn:partition:service:region:account-id:resource-id"`
- `"arn:partition:service:region:account-id:resource-type/resource-id"`
- `"arn:partition:service:region:account-id:resource-type:resource-id"`

Hinweis: Einige Dienste wie S3 verwenden Varianten wie arn:aws:s3: ::bucket-name (ohne Region oder Konto-ID).

OCSF-Status

Vorhandene

Beispiele

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
  ]
}
```

```
{
```

```
  "resources": [
    {
      "uid_alt": "arn:aws:s3:::my-bucket-name"
    }
  ]
}
```

Ressourcenname

Der eindeutige Name für die Cloud-Ressource.

Anforderung

Empfohlen

Typ

Zeichenfolge

Format

User-created Namen, deren Werte von der Umgebung abhängen.

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "name": "My-Server-1"
    }
  ]
}
```

Cloud-Region

Die AWS Region, in der sich die Ressource befindet.

Anforderung

Empfohlen

Typ

Zeichenfolge

Format

Gültiger Bezeichner der Cloud-Region (z. B. us-east-1, eu-west-1, ap-southeast-2)

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "region": "us-west-2"
    }
  ]
}
```

Zeit der Erstellung der Ressource

Der Zeitpunkt, zu dem die Ressource erstellt wurde.

Anforderung

Empfohlen

Typ

Zeitstempel

Format

Unix-Zeitstempel in Millisekunden seit der Epoche (1. Januar 1970, 00:00:00 UTC)

OCSF-Status

Vorhandene

Beispiel

```
{
```

```
  "resources": [
    {
      "created_time": 1762019193000
    }
  ]
}
```

Tags (Markierungen)

Key-value Paare für Ressourcenmetadaten und Organisation.

Anforderung

Empfohlen

Typ

Array von Key:Value-Objekten

Format

Ein generisches Objekt, mit dem ein Schlüssel/Wert-Paar definiert werden kann.

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "tags": [
        {
          "name": "Environment",
          "value": "Production"
        },
        {
          "name": "Owner",
          "value": "SecurityTeam"
        }
      ]
    }
  ]
```

```
}
```

IP-Adresse

Die der Instance zugeordnete IP-Adresse im IPv4- oder IPv6-Format.

Anforderung

Optional

Typ

Zeichenfolge

Format

Gültige IPv4- oder IPv6-Adresse

OCSF-Status

Vorhandene

Beispiel

```
{
  "resources": [
    {
      "ip": "10.0.1.25"
    }
  ]
}
```

IP-Adressen

Eine Reihe von IP-Adressen (IPv4 oder IPv6), die dem Gerät zugeordnet sind. Dazu können sowohl öffentliche als auch private IP-Adressen gehören.

Anforderung

Optional

Typ

Reihe von IP-Adressen

OCSF-Status

Neu

Beispiel

```
{
  "resources": [
    {
      "ip_addresses": ["10.0.1.25", "52.12.34.56"]
    }
  ]
}
```

VPC-UID

Die VPC-ID, in der sich die Ressource befindet.

Anforderung

Optional

Typ

Zeichenfolge

Format

VPC-ID (z. B. vpc-12345678900)

OCSF-Status

Hinzugefügt zu `resource_details`

Beispiel

```
{
  "resources": [
    {
      "vpc_uid": "vpc-0a1b2c3d4e5f6g7h8"
    }
  ]
```

```
}
```

Beispiel für ein Ressourcenobjekt mit grundlegenden Attributen

```
{
  "resources": [
    {
      "cloud_partition": "aws",
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      },
      "region": "us-east-1",
      "type": "AWS::EC2::NetworkInterface",
      "uid": "eni-03e6c892dd45e836c",
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-03e6c892dd45e836c",
      "zone": "us-east-1f",
      "vpc_uid": "vpc-0ef6045717b0362f6"
    }
  ]
}
```

Ressourcenspezifische Objekte

Dies sind komplexe verschachtelte Objekte, die detaillierte Informationen für bestimmte Ressourcentypen und Dienste bereitstellen. Jedes Objekt enthält mehrere Felder und Unterobjekte mit dienstspezifischer Konfiguration und Metadaten.

Gerät

Verbesserte Cloud-Instanz-Attribute für Rechenressourcen, einschließlich Verschlüsselungsdetails, Bildinformationen, Instanzprofil und Startzeit.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der Objektdefinition des OCSF-Geräts.

AWS Die Erweiterung fügt diesem Objekt die folgenden Attribute hinzu:

- `encryption_details`- Die Verschlüsselungsdetails der Ressource
- `image`- Bildinformationen
- `instance_profile`— Das IAM-Instanzprofil, das der Instance zugeordnet werden soll
- `launch_time`— Die Uhrzeit, zu der die Instance gestartet wurde
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource

Beispiel

```
{
  "device": {
    "image": {
      "uid": "ami-99999999",
      "name": "LoadTestAMI-Current"
    },
    "instance_profile": {
      "uid": "LoadTestingInstanceProfileId",
      "uid_alt": "arn:aws:iam::012345678999:instance-profile/generated"
    },
    "launch_time": 1762019193000,
    "launch_time_dt": "2025-08-02T02:05:06Z",
    "model": "m3.xlarge",
    "network_interfaces": [
      {
        "ip": "198.51.100.0",
        "security_groups": [
          {
            "name": "LoadTestingSecurityGroupName",
            "uid": "LoadTestingSecurityId"
          }
        ],
        "uid": "eni-abcdef12"
      }
    ],
```

```
    "type": "Virtual",
    "type_id": 6,
    "uid": "i-99999999"
  }
}
```

Netzwerkschnittstelle

Details und Konfiguration der Netzwerkschnittstelle, einschließlich Anlagen und Sicherheitsgruppen.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der Objektdefinition der OCSF-Netzwerkschnittstelle.

AWS Die Erweiterung fügt diesem Objekt die folgenden Attribute hinzu:

- `attachments`- Informationen zu den Anhängen an die Netzwerkschnittstelle
- `security_groups`- Reihe von eindeutigen Kennungen für Sicherheitsgruppen
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource

Beispiel

```
{
  "network_interface": {
    "uid": "eni-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a1b2c3d4e5f6g7h8",
    "name": "prod-web-server-eni",
    "attachments": [
      {
        "uid": "eni-attach-0abcd1234efgh5678",
```

```
        "instance_uid": "i-0123456789abcdef0",
        "name": "/dev/eth0",
        "state": "attached",
        "attach_time": 1762019193000
      }
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "web-server-sg"
      },
      {
        "uid": "sg-9i8h7g6f5e4d3c2b1",
        "name": "ssh-access-sg"
      }
    ]
  }
}
```

Speichergerät

Details zum Speichergerät, einschließlich Anlagen, Verschlüsselung und Snapshot-Informationen.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Neu

Das Speichergeräteobjekt umfasst die folgenden Attribute:

- `name`- Der Name des Speichergeräts
- `uid`- Die eindeutige Kennung des Speichergeräts
- `attachments`- Die Anhänge des Speichergeräts
- `encryption_details`- Der Verschlüsselungsschlüssel des Speichergeräts

- `is_encrypted`- Ob das Speichergerät verschlüsselt ist (erforderlich)
- `snapshot_id`- Die Snapshot-ID des Speichergeräts
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource

Beispiel

```
{
  "storage_device": {
    "is_encrypted": false,
    "name": "LocalVolumeDeviceName1",
    "snapshot_id": "snap-12345678901234567",
    "uid": "vol-09d5050dea915943d",
    "uid_alt": "arn:aws:ec2:us-west-2:123456789000:volume/vol-09d5050dea915943d"
  }
}
```

Datenbank

Attribute der Datenbank-Instance, einschließlich Engine-Typ, Endpunkt und Benutzerinformationen.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der Definition des https://schema.ocsf.io/1.6.0/objects/database OCSF-Datenbankobjekts.

AWS Die Erweiterung fügt diesem Objekt die folgenden Attribute hinzu:

- `cluster_uid`- Die Datenbank-Cluster-ID
- `db_endpoint`- Der Datenbank-Endpunkt
- `encryption_details`- Die Details zur Datenbankverschlüsselung
- `engine`- Der Name der Datenbank-Engine (z. B. mysql)

- `is_encrypted`- Ob die Datenbank verschlüsselt ist
- `is_iam_authentication`- Ob die IAM-Authentifizierung aktiviert ist
- `is_public`- Ob die Datenbank öffentlich zugänglich ist
- `port`- Die Portnummer der Datenbank
- `security_groups`- Array von VPC-Sicherheitsgruppen, die der Datenbankinstanz zugeordnet sind
- `snapshot_details`- Die Details des Datenbank-Snapshots
- `status`- Der Datenbankstatus (z. B. verfügbar)
- `subnet_group`— Eine Datenbank-Subnetzgruppe ist eine Sammlung von Subnetzen in einer VPC
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource
- `user`- Der Datenbankbenutzer
- `version`- Die Datenbankversion

Beispiel

```
{
  "database": {
    "cluster_uid": "SampleDBClusterId",
    "engine": "mysql",
    "is_iam_authentication": true,
    "is_public": false,
    "type": "Relational",
    "type_id": 1,
    "uid": "SampleDBId",
    "version": "13.6"
  }
}
```

Datenbank-Cluster

Attribute der Datenbankinstanz, einschließlich Engine-Typ, Endpunkt und Benutzerinformationen.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Neu

Das Datenbankobjekt enthält die folgenden Attribute:

- `uid`- Der eindeutige Bezeichner des Datenbank-Clusters
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource
- `name`— Der Name des Datenbank-Clusters
- `status`- Der Status des Datenbank-Clusters
- `engine`- Die dem Cluster zugeordnete Engine
- `version`- Die Version des Datenbank-Clusters
- `cluster_members`- Liste der Datenbankinstanzen, die Teil des Clusters sind
- `security_groups`- Reihe von Sicherheitsgruppen, die dem Cluster zugeordnet sind
- `is_encrypted`— Ob der Datenbank-Cluster verschlüsselt ist
- `is_iam_authentication`- Ob die IAM-Authentifizierung aktiviert ist
- `encryption_details`- Die Verschlüsselungsdetails des Datenbank-Clusters
- `subnet_group`- Die dem Cluster zugeordnete Subnetzgruppe
- `port`- Die Portnummer des Datenbank-Clusters
- `zones`- Liste der Verfügbarkeitszonen
- `db_endpoint`- Der Endpunkt des Datenbank-Clusters
- `snapshot_details`- Details des Datenbank-Snapshots

Beispiel

```
{
  "db_cluster": {
    "uid": "production-aurora-cluster",
    "uid_alt": "arn:aws:rds:us-east-1:123456789012:cluster:production-aurora-cluster",
    "name": "production-aurora-cluster",
    "status": "available",
```

```
    "engine": "aurora-mysql",
    "version": "8.0.mysql_aurora.3.04.0",
    "cluster_members": [
      "instance-1",
      "instance-2"
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "db-security-group"
      }
    ],
    "is_encrypted": true,
    "is_iam_authentication": true,
    "encryption_details": {
      "key_uid": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    "subnet_group": {
      "uid": "production-db-subnet-group"
    },
    "port": 3306,
    "zones": [
      "us-east-1a",
      "us-east-1b",
      "us-east-1c"
    ],
    "db_endpoint": {
      "name": "production-aurora-cluster.cluster-abc123xyz.us-
east-1.rds.amazonaws.com",
      "port": 3306
    }
  }
}
```

Cloud-Funktion

Cloud-Funktionsattribute für serverlose Funktionen, einschließlich Handler, Ebenen und Laufzeitkonfiguration.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Neu

Das Cloud-Funktionsobjekt umfasst die folgenden Attribute:

- `name`- Der Name der Cloud-Funktion
- `uid`- Die eindeutige Kennung der Cloud-Funktion
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource
- `encryption_details`— Die Verschlüsselungsdetails der Cloud-Funktion
- `handler`- Die Methode im Funktionscode, die Ereignisse verarbeitet
- `layers`- Die Liste der Cloud-Funktionsebenen, die zusätzlichen Code oder Daten enthalten
- `runtime`- Die sprachspezifische Umgebung der Cloud-Funktion
- `security_groups`- Reihe von Sicherheitsgruppen, die der Cloud-Funktion zugeordnet sind
- `subnet_info_list`- Details zu Subnetzen, die mit der Cloud-Funktion verknüpft sind
- `user`— Details zur IAM-Entität, die der cloud_function die Berechtigung für den Zugriff auf Dienste erteilt
- `version`— Die Version der Cloud-Funktion
- `vpc_uid`- Die eindeutige Kennung der VPC, wenn sich die Cloud-Funktion in einer VPC befindet

Beispiel

```
{
  "cloud_function": {
    "name": "my-lambda-function",
    "uid": "my-lambda-function",
    "uid_alt": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function",
    "handler": "index.handler",
    "runtime": "python3.11",
    "version": "$LATEST",
    "layers": [
      {
        "name": "my-layer",
```

```
        "uid_alt": "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1",
        "version": "1"
      }
    ],
    "security_groups": [
      {
        "name": "lambda-security-group",
        "uid": "sg-0123456789abcdef0"
      }
    ],
    "subnet_info_list": [
      {
        "uid": "subnet-0a1b2c3d4e5f6g7h8"
      }
    ],
    "vpc_uid": "vpc-0ef6045717b0362f6"
  }
}
```

Datenpaket

S3-Bucket- oder Datenspeicherattribute.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der OCSF-Databucket-Objektdefinition.

Hinweis: Dieses Objekt wird von der Erweiterung zu resource_details hinzugefügt. AWS Das OCSF-Databucket-Kernobjekt wird ohne zusätzliche Attribute verwendet.

Beispiel

```
{
```

```
  "databucket": {
    "type": "S3",
    "type_id": 1,
    "uid": "my-bucket-name"
  }
}
```

Image

Bildinformationen für Rechenressourcen, einschließlich Plattform- und Nutzungsdetails.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der Definition des https://schema.ocsf.io/1.6.0/objects/image OCSF-Bildobjekts.

AWS Die Erweiterung fügt diesem Objekt die folgenden Attribute hinzu:

- `platform`- Die Betriebssystemplattform des Images
- `in_use_count`- Anzahl der Ressourcen, die dieses Image verwenden

Beispiel

```
{
  "image": {
    "uid": "ami-0abcdef1234567890",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:image/ami-0abcdef1234567890",
    "name": "my-custom-ami",
    "platform": "AMAZON_LINUX_2",
    "in_use_count": 2
  }
}
```

Informationen zum Subnetz

Details über das Subnetz, in dem sich die Ressource befindet.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Neu

Das Subnetz-Info-Objekt enthält die folgenden Attribute:

- `uid`- Die eindeutige Kennung des Subnetzes
- `uid_alt`— Amazon-Ressourcenname (ARN) der Ressource
- `name`— Der Name des Subnetzes
- `zone`- Die Verfügbarkeitszone
- `ip_count`- Die Anzahl der IP-Adressen im Subnetz
- `cidr_block`- Der CIDR-Block des Subnetzes
- `is_default`- Ob dies das Standardsubnetz ist
- `is_public`- Ob das Subnetz öffentlich zugänglich ist
- `state`- Der Status des Subnetzes
- `vpc_uid`- Die VPC-ID, in der sich das Subnetz befindet

Beispiel

```
{
  "subnet_info": {
    "uid": "subnet-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a1b2c3d4e5f6g7h8",
    "name": "production-web-subnet-1a",
    "zone": "us-east-1a",
    "ip_count": 251,
    "cidr_block": "10.0.1.0/24",
    "is_default": false,
```

```
    "is_public": true,
    "state": "available",
    "vpc_uid": "vpc-0123456789abcdef0"
  }
}
```

Benutzer

IAM-Benutzerattribute, einschließlich Instanzprofile und Richtlinien.

Anforderung

Optional

Typ

Objekt

OCSF-Status

Hinzugefügt zu. `resource_details` Weitere Informationen finden Sie in der Definition des https://schema.ocsf.io/1.6.0/objects/user OCSF-Benutzerobjekts.

Das Benutzerobjekt enthält die folgenden Attribute:

- `instance_profiles`— Liste der Instanzprofile, die an eine Cloud-Instanz angehängt sind
- `policies`- Richtlinien, die Benutzern, Gruppen, Rollen und Ressourcen Berechtigungen zuweisen

Beispiel

```
{
  "user": {
    "type_id": 1,
    "uid": "AIDACKCEVSQ6C2EXAMPLE",
    "uid_alt": "arn:aws:iam::123456789012:user/developers/john.doe",
    "name": "john.doe",
    "type": "User",
    "groups": [
      {
        "name": "Developers"
      },
      {
```

```
        "name": "ReadOnlyAccess"
      }
    ],
    "policies": [
      {
        "name": "AmazonS3ReadOnlyAccess"
      },
      {
        "name": "AmazonEC2ReadOnlyAccess"
      }
    ]
  }
}
```

Ergebnisse der Berichterstattung in Security Hub

Die Ergebnisse der Sicherheitsabdeckung für Security Hub geben Aufschluss AWS darüber, welche Sicherheitsfunktionen aktiviert sind und wo Lücken in der Abdeckung in einem eigenständigen Konto oder in den Mitgliedskonten einer Organisation bestehen könnten. Die Ergebnisse der Berichterstattung unterstützen derzeit die Berichterstattung darüber, welche Dienste und Funktionen für Amazon GuardDuty, Amazon Inspector, Amazon Macie und AWS Security Hub CSPM aktiviert sind. Diese Erkenntnisse werden im Widget „Sicherheitsabdeckung“ auf dem Security Hub-Dashboard angezeigt und bieten die Möglichkeit, detailliertere Ansichten nach bestimmten Sicherheitsfunktionen aufzurufen.

Einschränkungen

- Für Mitgliedskonten werden die Deckungsinformationen für alle verknüpften Konten zusammengefasst AWS-Regionen, jedoch nur für dieses Mitgliedskonto.
- Für Konten, die nicht bei Security Hub registriert sind, werden keine Deckungsinformationen angezeigt.

Ergebnisse der Netzabdeckung für AWS Security Hub CSPM

Mit den Ergebnissen der Security Hub CSPM-Abdeckung wird bewertet, ob in einem Konto ein qualifizierter Sicherheitsstandard für das Statusmanagement aktiviert ist. Die Aktivierung eines beliebigen Security Hub CSPM-Standards gilt als qualifiziert, mit Ausnahme der Resource AWS Control Tower Tagging-Standards.

Bei der Aktivierung von Security Hub CSPM kann es bis zu 24 Stunden dauern, bis die standardmäßig aktivierten Standards erkannt werden.

Ergebnisse der Berichterstattung für Amazon GuardDuty

GuardDuty Anhand der Ergebnisse der Netzabdeckung GuardDuty wird bewertet, ob und welche GuardDuty Funktionen in einem der folgenden Fälle aktiviert sind AWS-Konto:

- GuardDuty Malware-Schutz für Amazon EC2 — Scannt Amazon EC2-Instances nach potenzieller Malware.
- GuardDuty Amazon EKS-Schutz — Überwacht die Kubernetes-Auditprotokolle auf Bedrohungen in Amazon EKS-Clustern.
- GuardDuty Lambda-Schutz — Analysiert Aufrufe von Lambda-Funktionen auf potenzielle Bedrohungen.
- GuardDuty Amazon S3-Schutz — Analysiert Datenereignisse im Hinblick auf potenzielle Bedrohungen für Amazon S3-Buckets.
- GuardDuty Amazon RDS-Schutz — Überwacht Amazon RDS-Datenbanken auf Bedrohungen.
- GuardDuty Laufzeitüberwachung — Ermöglicht die Überwachung des Laufzeitverhaltens in Amazon EC2-Instances in Echtzeit.
- GuardDuty Grundlegende Abdeckung — GuardDuty Basisfunktionen, die automatisch aktiviert werden, wenn sie GuardDuty aktiviert sind.

> **Note**
>
> Bei GuardDuty der Basisabdeckung bedeuten Ergebnisse, die darauf hinweisen, dass die Funktion deaktiviert ist, dass das Konto für das Deckungsergebnis nicht aktiviert GuardDuty ist.

Es kann bis zu 24 Stunden dauern, bis Aktualisierungen des GuardDuty Versicherungsschutzes für alle Mitgliedskonten einer Organisation übernommen werden.

Ergebnisse der Berichterstattung für Amazon Inspector

Anhand der Ergebnisse von Amazon Inspector wird bewertet, ob Amazon Inspector aktiviert ist und welche Funktionen in einem Konto aktiviert sind:

- Inspector EC2 Scanning — Scannt Amazon EC2-Instances auf Sicherheitslücken.
- Inspector ECR Scanning — Scannt Amazon ECR-Container-Images auf Sicherheitslücken.
- Inspector Lambda Standard Scanning — Scannt Lambda-Funktionen nach Sicherheitslücken.
- Inspector Lambda Code Scanning — Scannt Lambda-Code-Funktionen auf Code-Schwachstellen.

Ergebnisse der Berichterstattung für Amazon Macie

Anhand der Ergebnisse der Macie-Abdeckung wird bewertet, ob Macie für folgende Bereiche aktiviert ist: AWS-Konten

- Macie Automated Sensitive Data Discovery Coverage — Evaluiert Ihren Amazon S3-Datenbestand kontinuierlich auf sensible Daten.

Es kann bis zu 24 Stunden dauern, bis die automatische Erkennung sensibler Daten durch Macie aktualisiert wird, bis die Ergebnisse der Abdeckung für alle Mitgliedskonten in einer Organisation übernommen werden.

Ergebnisse der Berichterstattung werden unterdrückt

Standardmäßig wird anhand der Ergebnisse der Sicherheitsabdeckung bewertet GuardDuty, welche CSPM-Funktionen von Amazon, Amazon Inspector, Amazon Macie und AWS Security Hub für ein Konto und eine Region aktiviert sind. Wenn bestimmte Sicherheitsfunktionen für Sie nicht geeignet sind oder ein akzeptiertes Risiko darstellen, können Sie die Sperrfunktion verwenden, um Deckungsfeststellungen ähnlich wie alle anderen Ergebnisse zu unterdrücken. Wenn ein Deckungsergebnis unterdrückt wird, wird es nicht in die Deckungsberechnungen im Widget „Sicherheitsabdeckung“ einbezogen. Das Widget zeigt die folgende Meldung an: Die Deckung von Sicherheitsfunktionen wurde aufgrund der Ergebnisse der unterdrückten Deckung ausgeschlossen. Die Meldung enthält die Anzahl der unterdrückten Ergebnisse.

Um ein Abdeckungsergebnis in Security Hub zu unterdrücken

1. Wenn Sie das Widget „Sicherheitsabdeckung“ aufrufen, wählen Sie den Link „Prozentsatz der abgedeckten Bereiche“ aus.
2. Wählen Sie im Popup-Fenster „Deckung anzeigen“ die Option „Ergebnisse der Berichterstattung anzeigen“ aus. Jedes Ergebnis mit dem Status „Neu“ weist auf eine beobachtete Deckungslücke hin.

3. Aktivieren Sie das Kontrollkästchen neben jedem Ergebnis, das Sie unterdrücken möchten.
4. Wählen Sie oben auf der Seite die Option Status aktualisieren und dann Unterdrückt aus.
5. Geben Sie im Dialogfeld „Status auf Unterdrückt setzen“ optional eine Notiz ein, in der der Grund für die Statusänderung detailliert beschrieben wird. Wählen Sie dann „Status festlegen“.

KI-Inventar im Security Hub

Das KI-Inventar in AWS Security Hub bietet einen einheitlichen Überblick über Ihre Ressourcen für künstliche Intelligenz (KI) und maschinelles Lernen (ML) in Ihrer gesamten AWS Umgebung. Verwenden Sie das KI-Inventar, um nicht genehmigte KI-Workloads zu identifizieren, zu verstehen, wo KI läuft und wie sie entdeckt wurde, und um die Ressourcen zu priorisieren, die einer genaueren Sicherheitsüberprüfung bedürfen. Security Hub unterteilt KI-Ressourcen in zwei Erkennungstypen:

- Verwaltet — KI-Ressourcen, die AWS als verwalteter Dienst bereitgestellt werden. Security Hub erkennt diese Ressourcen anhand von AWS Config Konfigurationselementen. Zu den verwalteten Ressourcentypen gehört eine unterstützte Teilmenge von Amazon Bedrock, Amazon Bedrock AgentCore und Amazon. SageMaker
- Self-hosted— KI-Ressourcen, die nicht als verwalteter Service bereitgestellt werden. Beispiele hierfür sind Open-Source-Modelle, Agenten und Inferenzserver, die auf Ihrem eigenen Computer ausgeführt werden. Security Hub erkennt, dass diese Ressourcen Signale auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Amazon Elastic Container Registry (Amazon ECR) -Images beitragen. Zu den Signalen gehören die Ergebnisse der Amazon Inspector-Software Bill of Materials (SBOM) und GuardDuty Amazon-DNS-Aktivitäten.

Administratorkonten können KI-Ressourcen von allen aktivierten Konten in ihrer Organisation aus einsehen. Mitgliedskonten können nur die KI-Ressourcen in ihrem eigenen Konto anzeigen.

Voraussetzungen für die selbst gehostete KI-Erkennung

Für die Erkennung verwalteter KI-Ressourcen ist keine zusätzliche Konfiguration erforderlich, die über die Aktivierung von Security Hub hinausgeht. Um selbst gehostete KI-Ressourcen zu finden, müssen Sie auch diejenigen aktivieren AWS-Services , die die entsprechenden Signale liefern:

- Amazon Inspector — Aktivieren Sie Amazon Inspector (mit Security Hub Hub-Grundlagen), um SBOMs zu generieren. Security Hub verwendet diese SBOMs, um selbst gehostete Modelle, Inferenzendpunkte und Agenten zu erkennen. Aktivieren Sie für Amazon EC2 EC2-Instances

agentenbasiertes Scannen mit erweitertem Scanmodus, agentenloses Scannen oder Hybrid-Scannen. Agent-based Beim Scannen ohne erweiterten Scanmodus wird nicht das umfangreiche Softwareinventar erzeugt, das für die KI-Ressourcenerkennung erforderlich ist. Für Amazon ECR-Images stellt Amazon Inspector SBOMs durch Scannen von Container-Images bereit.

- Amazon GuardDuty — Aktivieren Sie diese GuardDuty Option, damit Security Hub DNS-Aktivitäten verwenden kann, um externe KI-Endpunkte zu erkennen, die Ihre Amazon EC2 EC2-Instances aufrufen.

Unterstützte KI-Ressourcentypen

Sofern allgemein verfügbar, unterstützt Security Hub die folgenden selbst gehosteten KI-Ressourcentypen. Security Hub verwendet ein vertrauensbasiertes Erkennungssystem für selbst gehostete KI-Ressourcen. Jede Erkennung ist in einem Primärsignal verankert, z. B. einer SBOM-Komponente. Security Hub korreliert dann zusätzliche Signale, um Vertrauen herzustellen, bevor eine Ressource in Ihrem Inventar erscheint. Security Hub zeigt nur die Ressourcen an, die den Konfidenzschwellenwert erreichen, wodurch Fehlalarme minimiert werden. Jede Ressource verwendet ein `ResourceType` mit dem `SelfHosted::AI::` Präfix.

- Modelle (`SelfHosted::AI::Model`) — Modelle Hugging Face und Ollama. Security Hub erkennt Modelle nur in den Standard-Modell-Cache-Verzeichnissen (wie den Hugging Face- und Ollama-Caches) und in benutzerdefinierten Pfaden, die Sie für das Scannen mit Amazon Inspector konfigurieren.
- Inferenzendpunkte (`SelfHosted::AI::InferenceEndpoint`) — Unterstützte Model-Serving-Software wie VllM, Ollama TorchServe, Triton, Text Generation Inference (TGI), SGLang, llama.cpp, LocalAI, BentoML, Xference, Ray Serve und GPT4All.
- Agenten `SelfHosted::AI::Agent` () OpenClaw — Agenten.
- Externe Endpunkte (`SelfHosted::AI::ExternalEndpoint`) — Externe KI-Servicedomänen, die Ihre Amazon EC2 EC2-Instances aufrufen. Security Hub verwaltet eine Zulassungsliste mit bekannten KI-Servicedomänen wie OpenAI, Anthropic, Cohere, Mistral und anderen wichtigen KI-Anbietern und erkennt, wenn Ihre Instances DNS-Anfragen an sie stellen. Externe Endpunkte werden nur anhand von GuardDuty DNS-Aktivitäten auf Amazon EC2 erkannt.

Verwaltete KI-Ressourcen sind eine unterstützte Untergruppe der SageMaker Konfigurationselementtypen Amazon Bedrock AgentCore, Amazon Bedrock und Amazon, jeweils mit der `AI/ML` Ressourcenkategorie.

Suchen nach KI-Ressourcen auf der Seite „Ressourcen“

Auf der Seite Ressourcen werden alle Ressourcen in Ihrer Umgebung aufgeführt. Bei KI-Ressourcen können Sie die folgenden Funktionen verwenden, um KI-Workloads und die Hosts, auf denen sie ausgeführt werden, zu identifizieren:

- Bei verwalteten AI/ML Ressourcen wird neben der Ressource ein KI-Symbol angezeigt. Wählen Sie das Symbol, um eine Beschreibung anzuzeigen.
- Host-Ressourcen, auf denen selbst gehostete KI-Ressourcen ausgeführt werden, wie Amazon EC2 EC2-Instances, zeigen ein selbst gehostetes AI-Zählsymbol. Hosts ohne selbst gehostete KI-Ressourcen zeigen kein Badge an.
- Verwende den Schnellfilterschalter, um nur die Hosts anzuzeigen, die selbst gehostete KI-Ressourcen enthalten.
- Um einen Host genauer zu untersuchen, wählen Sie den Host aus, um seinen Detailbereich zu öffnen, wählen Sie die Registerkarte KI-Assets und dann Alle anzeigen aus, um die auf diesem Host erkannten selbst gehosteten KI-Ressourcen zu sehen.

Verwenden Sie die KI-Inventarseite

Die KI-Inventarseite konzentriert sich auf die KI-Ressourcen in Ihrem Unternehmen. Jede Ressource auf dieser Seite gehört zur `AI/ML` Ressourcenkategorie. Auf dieser Seite werden verwaltete AWS KI-Ressourcen und selbst gehostete KI-Ressourcen in Ihrer Umgebung angezeigt. In den folgenden Abschnitten werden die Hauptkomponenten der Seite beschrieben.

Übersichtsleiste

In der Übersichtsleiste werden die Gesamtzahl der KI-Assets sowie eine Aufschlüsselung nach Erkennungstyp angezeigt, entweder selbst gehostet oder verwaltet. Außerdem wird eine Aufschlüsselung nach Unterkategorien wie Modell oder Agent angezeigt. Wählen Sie den Wert für eine Statistik aus, um die unterstützenden Details in der Tabelle anzuzeigen.

Gruppieren, Filtern und Suchen

In der AI-Inventartabelle werden Ressourcen standardmäßig nach Ressourcentyp gruppiert. Sie können die Gruppierung ändern oder entfernen, um eine flache Ansicht aller Ressourcen zu erhalten. Zu den verfügbaren Gruppierungsfeldern gehören die kanonische ID, der Hostressourcentyp, der Ermittlungstyp, die Konto-ID und der Ressourcentyp.

Die kanonische ID identifiziert, was eine Ressource ist, unabhängig davon, wo sie ausgeführt wird. Beispielsweise verwenden zwei Amazon EC2 EC2-Instances, die dasselbe Hugging Face Face-Modell ausführen, dieselbe kanonische ID, sodass Sie alle Bereitstellungen eines bestimmten Modells in Ihrer Organisation finden können.

> **Note**
>
> Die Gruppierungen mit der kanonischen ID und dem Host-Ressourcentyp gelten nur für selbst gehostete Ressourcen. Wenn Sie nach diesen Feldern gruppieren, werden verwaltete KI-Ressourcen nicht in den Ergebnissen angezeigt, da sie diese Attribute nicht haben. Verwenden Sie Gruppierungen vom Typ Discovery oder vom Ressourcentyp, um sowohl verwaltete als auch selbst gehostete Ressourcen zusammen anzuzeigen.

Schnellfilter ermöglichen das Filtern nach einer Ressourcenunterkategorie oder einem Discovery-Typ. Eigenschaftsfilter unterstützen zusätzliche Felder, darunter den Host-Ressourcentyp und die kanonische ID für selbst gehostete Ressourcen.

Details zu Ressourcen und beitragende Signale

Wählen Sie eine Ressourcenzeile aus, um den Detailbereich zu öffnen. Für verwaltete Ressourcen zeigt das Panel die Ressourcenkonfiguration als JSON an. Bei selbst gehosteten Ressourcen zeigt das Panel die beitragenden Signale an, die Security Hub zur Erkennung der Ressource verwendet hat. Zu diesen Signalen gehören die Erkennungsquelle und einzelne Signaldetails, z. B. die SBOM-Komponenten und die unterstützende Inferenzsoftware für ein Modell oder die DNS-Domäne für einen externen Endpunkt.

Ein Rollup zur Host-Ressource

Bei einer selbst gehosteten KI-Ressource wird im Detailbereich die Host-Ressource angezeigt, auf der Security Hub die Ressource erkannt hat. Um alle selbst gehosteten KI-Ressourcen auf demselben Host zu sehen, filtern Sie die Tabelle nach der Host-Ressource. In dieser Ansicht können Sie von einer einzelnen selbst gehosteten Ressource einen Drillup zu ihrem Host durchführen und die angrenzenden KI-Ressourcen auf diesem Host überprüfen.

Überlegungen

Für das KI-Inventar gelten bei allgemeiner Verfügbarkeit die folgenden Einschränkungen:

- Self-hosted KI-Ressourcen enthalten in dieser Version keine Ergebnisse. Security Hub zeigt nur die Anzahl der Ergebnisse für verwaltete KI-Ressourcen an.
- Self-hosted Die KI-Erkennung wird nur auf Amazon EC2 EC2-Instances und Amazon ECR-Images unterstützt. AWS Lambda Funktionen und andere Berechnungstypen werden nicht unterstützt.
- Security Hub ordnet Amazon ECR-Images in dieser Version keinem übergeordneten Host zu, sodass sie in der Anzahl der Host-KI nicht enthalten sind.
- Security Hub erkennt externe Endpunkte nur anhand von GuardDuty DNS-Aktivitäten auf Amazon EC2. In dieser Version ordnet Security Hub keine Aufrufe von AWS Fargate, Amazon AWS Lambda SageMaker, Amazon EKS oder anderen service-verwalteten Rechnern zu.

Mit der API auf das KI-Inventar zugreifen

Mit der GetResourcesV2 und den Vorgängen können Sie KI-Inventardaten programmgesteuert abrufen. GetResourcesStatisticsV2

Bei AI/ML Ressourcen umfasst die `GetResourcesV2` Antwort die Felder `ResourceSubCategory` und`DiscoveryType`. Das `DiscoveryType` Feld gibt an, ob es sich bei einer Ressource um `Managed` oder handelt`SelfHosted`. Bei selbst gehosteten KI-Ressourcen und ihren Host-Ressourcen beinhaltet `ResourceInfo` die Antwort auch eine `AIDetails` Struktur.

Self-hosted KI-Ressourcen verwenden a `ResourceType` mit dem `SelfHosted::AI::` Präfix. Zu den unterstützten Typen gehören die folgenden:

- `SelfHosted::AI::Model`
- `SelfHosted::AI::Agent`
- `SelfHosted::AI::InferenceEndpoint`
- `SelfHosted::AI::ExternalEndpoint`

Die `AIDetails` Struktur verknüpft eine selbst gehostete KI-Ressource mit ihrem Host mithilfe der `HostResourceType` Felder `HostResourceGuid` und. Das `CanonicalId` Feld identifiziert, was eine Ressource ist, unabhängig davon, wo sie bereitgestellt wird, sodass Sie identische Ressourcen auf mehreren Hosts zusammenfassen können. Die kanonische ID verwendet ein `type/identifier` Format:

- Für ML-Modelle: `model/<purl>` (zum Beispiel) `model/pkg:huggingface/meta-llama/llama-3-8b`

- Für Inferenzendpunkte und Agenten: ein Format `type/asset-identifier-name`
- Für externe Endpunkte: die normalisierte Domäne (zum Beispiel) `api.*.openai.com`

Auf einer Host-Ressource, z. B. einer Amazon EC2 EC2-Instance, enthalten die `SelfHostedAI*ResourceCount` Felder und das `SelfHostedTotalAIResourceCount` Feld die Anzahl der selbst gehosteten KI-Ressourcen, die auf dem Host erkannt wurden.

Note

Wenn Sie verwenden `GetResourcesV2` und nach filtern`ResourceSubCategory`, müssen Sie auch einen `ResourceCategory` Filter angeben. Stellen Sie den Vergleich auf `EQUALS` und den Wert auf`AI/ML`. Diese Anforderung gilt auch, wenn Sie nach `ResourceSubCategoryResourceInfo.AIDetails.HostResourceType`, oder `ResourceInfo.AIDetails.CanonicalId` in gruppieren`GetResourcesStatisticsV2`. Andernfalls gibt die Operation a zurück`ValidationException`.
Das folgende Beispiel zeigt eine gültige Filterkombination:

```
{
    "Filters": {
        "CompositeFilters": [
            {
                "Operator": "AND",
                "StringFilters": [
                    {
                        "FieldName": "ResourceCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "AI/ML"
                        }
                    },
                    {
                        "FieldName": "ResourceSubCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "Model"
                        }
                    }
                ]
            }
        ]
```

```
    }
}
```

Ressourcen im Security Hub

Security Hub weist jeder Ressource in Ihrer Umgebung eine Kritikalitätsstufe zu. Die Kritikalität gibt an, wie wichtig eine Ressource für Ihr Unternehmen ist, und hilft Ihnen dabei, Sicherheitsaufgaben zu priorisieren. Kritikalität ist eine von`Very High`,, `High``Medium`, `Low` oder. `Unknown`

Wie Security Hub auf Kritikalität schließen kann

Standardmäßig leitet Security Hub die Kritikalität aus Signalen auf der Ressource ab:

- Ressourcenname — Security Hub stimmt mit Mustern im Ressourcennamen überein. Beispielsweise wird eine Ressource mit `pci` oder `prod` in ihrem Namen als wichtiger behandelt als eine Ressource mit dem Namen`sandbox`.
- Tags — Security Hub gleicht Mustern in Ressourcen-Tags ab. Beispielsweise wird eine Ressource, die mit markiert `environment=production` ist, als wichtiger behandelt als eine Ressource mit einem Tag`environment=dev`.

Überschreiben der Kritikalität mit einer Automatisierungsregel

Sie können die abgeleitete Priorität außer Kraft setzen, indem Sie eine Automatisierungsregel erstellen, die die Priorität explizit für Ressourcen festlegt, die den Kriterien der Regel entsprechen. Eine Automatisierungsregel hat immer Vorrang vor der abgeleiteten Kritikalität. Weitere Informationen finden Sie unter Aktionen und Kriterien für Ressourcenregeln.

Wie wirkt sich Kritikalität auf den Schweregrad der Expositionsfindung

Security Hub verwendet die Ressourcenkritikalität als Eingabe, wenn es die Auswirkungen und den Schweregrad einer Risikofeststellung berechnet. Ressourcen mit einer Kritikalität von haben `Unknown` keinen Einfluss auf den Schweregrad der Expositionsfeststellung. Weitere Informationen finden Sie unter Auswirkung.

Erkenntnisse zu Sicherheitsrisiken in Security Hub

Ein Sicherheitsrisiko in Security Hub stellt die Korrelation mehrerer Sicherheitssignale dar, die potenzielle Sicherheitsrisiken in Ihrer AWS Umgebung identifizieren. Die Ergebnisse der Sicherheitsrisiken helfen Ihnen dabei, Sicherheitsrisiken zu verstehen und zu priorisieren. Sie analysieren automatisch Kombinationen von Sicherheitslücken, Konfigurationen, Bedrohungen und Ressourcenbeziehungen. Ein Expositionsbefund umfasst Merkmale und Signale. Ein Signal kann eine oder mehrere Arten von Expositionsmerkmalen enthalten. Security Hub generiert eine Risikofeststellung, wenn Signale von Security Hub CSPM, Amazon Inspector GuardDuty, Macie oder anderen AWS Diensten auf das Vorliegen einer Gefährdung hinweisen. Eine Ressource kann bei höchstens einem Expositionsergebnis die Hauptressource sein. Wenn eine Ressource keine oder nur unzureichende Expositionsmerkmale aufweist, generiert Security Hub keine Expositionsfeststellung für diese Ressource.

Wie funktionieren Expositionsergebnisse

Security Hub generiert Ergebnisse zur Gefährdung durch:

Analyse von Signalen von mehreren AWS Sicherheitsdiensten

Security Hub sammelt und analysiert kontinuierlich Sicherheitssignale von mehreren AWS Sicherheitsdiensten. Es erfasst Ergebnisse von GuardDuty zur Bedrohungserkennung, Amazon Inspector zur Schwachstellenbeurteilung, Security Hub CSPM für Konfigurationsprüfungen und Macie zur Offenlegung sensibler Daten. Diese Signale werden mithilfe fortschrittlicher Korrelations-Engines verarbeitet, um potenzielle Sicherheitsrisiken zu identifizieren.

Bewertung von Ressourcenkonfigurationen und -beziehungen

Das System führt eine detaillierte Bewertung der Ressourcenkonfigurationen anhand bewährter Sicherheitsverfahren durch. Es untersucht dienstspezifische Einstellungen, Compliance-Anforderungen und Sicherheitskontrollen. Diese Analyse hilft dabei, Fehlkonfigurationen zu identifizieren, die in Kombination mit anderen Faktoren zu Sicherheitslücken führen könnten.

Bewertung der Erreichbarkeit des Netzwerks

Ein entscheidender Bestandteil der Feststellungen zur Exposition ist die Bewertung der Erreichbarkeit der Netze. Das System bewertet sowohl die Internetgefährdung als auch die internen Netzwerkzugangspfade. Es analysiert Sicherheitsgruppenkonfigurationen und Netzwerk-ACL-Einstellungen, um potenzielle Angriffsvektoren zu ermitteln. Diese Analyse hilft dabei, Ressourcen zu identifizieren, die versehentlich unbefugten Zugriffen ausgesetzt sein könnten.

Korrelierung verwandter Sicherheitsprobleme

Die Korrelationsengine bildet die Beziehungen zwischen AWS Ressourcen ab, analysiert, wie sie interagieren, und identifiziert potenzielle Sicherheitsauswirkungen. Es untersucht IAM-Berechtigungen, Rollen und Ressourcenzugriffsmuster, um den breiteren Sicherheitskontext zu verstehen. Dieser Prozess hilft dabei, Sicherheitsrisiken zu identifizieren, die aufgrund der Kombination scheinbar harmloser Einzelkonfigurationen bestehen könnten.

Bestandteile einer Risikofeststellung

Jeder Expositionsergebnis umfasst:

Titel und Beschreibung des potenziellen Sicherheitsrisikos

Jedes gefundene Risiko enthält einen klaren, beschreibenden Titel, der unmittelbar die Art des Sicherheitsrisikos vermittelt. Die Beschreibung enthält detaillierte Informationen über die potenziellen Auswirkungen auf die Sicherheit, die betroffenen Ressourcen und den breiteren Kontext des Risikos. Diese Informationen helfen Sicherheitsteams dabei, das Risiko schnell zu verstehen und einzuschätzen.

Klassifizierung des Schweregrads (Kritisch, Hoch, Mittel, Niedrig)

- Der Schweregrad „Kritisch“ bedeutet, dass aufgrund der hohen Wahrscheinlichkeit eines Exploits und der erheblichen potenziellen Auswirkungen sofortige Maßnahmen erforderlich sind. Bei diesen Ergebnissen handelt es sich in der Regel um leicht auffindbare und ausnutzbare Sicherheitslücken.
- Ein hoher Schweregrad deutet darauf hin, dass mit mäßiger bis hoher Wahrscheinlichkeit und erheblichen potenziellen Auswirkungen vordringliche Maßnahmen erforderlich sind. Diese Ergebnisse sind möglicherweise relativ einfach auszunutzen, erfordern jedoch möglicherweise besondere Bedingungen.
- Ein mittlerer Schweregrad bedeutet, dass planmäßige Maßnahmen erforderlich sind, die Wahrscheinlichkeit eines Exploits geringer ist und die potenziellen Auswirkungen moderat sind. Diese Ergebnisse erfordern in der Regel komplexere Ausnutzungsmethoden.
- Ein niedriger Schweregrad deutet darauf hin, dass routinemäßige Maßnahmen erforderlich sind, da das Nutzungspotenzial begrenzt ist und die Auswirkungen gering sind. Diese Ergebnisse sind in der Regel schwer auszunutzen und bergen ein minimales Risiko.

Merkmale, die zur Exposition beigetragen haben

Einflussfaktoren sind die wichtigsten Faktoren, die zur Feststellung der Exposition geführt haben. Zu den beitragenden Merkmalen gehören die folgenden:

- Direkte Sicherheitslücken
- Konfigurationsprobleme
- Bedingungen der Netzwerkexposition
- Einstellungen für Ressourcenberechtigungen
- Ressourcenkritikalität (die Bedeutung einer Ressource für das Unternehmen)

Jedes Merkmal enthält spezifische Informationen darüber, wie es zum allgemeinen Sicherheitsrisiko beiträgt.

Visualisierung des potenziellen Angriffspfads und des Explosionsradius

Der potenzielle Angriffspfad und die Visualisierung des Explosionsradius bieten ein interaktives Diagramm, das zeigt, wie potenzielle Angreifer die identifizierte Gefahr ausnutzen könnten. Es ordnet Ressourcenbeziehungen, Netzwerkpfade und Pfade zur Rechteerweiterung nachgelagerten Ressourcen zu, auf die ein Angreifer potenziell zugreifen kann, wenn die Sicherheitslücke ausgenutzt wird.

Detaillierte Anleitungen zur Problembehebung

Jede festgestellte Exposition umfasst ausführliche Hinweise zur Behebung der identifizierten Risiken mit spezifischen, umsetzbaren Maßnahmen. Diese Anleitung umfasst Empfehlungen für bewährte Verfahren, Schritte zur Konfigurationskorrektur und priorisierte Maßnahmen. Die Leitlinien sind auf das spezifische Expositionsszenario zugeschnitten und berücksichtigen die beteiligten AWS Dienste.

Einzelheiten zur Konfiguration der Ressourcen

Konfiguration der Ressource zum Zeitpunkt der Erstellung des Ergebnisses sowie aktuelle Konfiguration der Ressource im Security Hub Hub-Ressourceninventar-Dashboard.

Kontextuelle Merkmale bieten zusätzlichen Sicherheitskontext

Kontextuelle Merkmale sind zusätzliche Sicherheitsmarkierungen, die von Security Hub identifiziert, aber nicht zur Erstellung eines Risikos verwendet wurden.

Ungenutzte Zugriffsinformationen aus dem IAM Access Analyzer können als kontextuelle Merkmale in Risikoergebnissen erscheinen. Wenn eine einer Ressource zugeordnete IAM-Rolle über

ungenutzte Berechtigungen verfügt, nimmt Security Hub diese Informationen als kontextuelles Merkmal in die Expositionsdetailansicht auf. Wenn beispielsweise eine Amazon EC2 EC2-Instance eine Softwareschwachstelle aufweist und die ihr zugeordnete IAM-Rolle 47 ungenutzte Berechtigungen für 5 Services hat, zeigt das Exposure Befund die ungenutzten Berechtigungen als zusätzlichen Kontext an. Dies hilft Ihnen, den potenziellen Explosionsradius zu verstehen — eine anfällige Ressource mit einer überprivilegierten IAM-Rolle stellt ein höheres Risiko dar als eine Ressource mit den geringsten Rechten, da eine kompromittierte Ressource diese ungenutzten Berechtigungen verwenden könnte, um den Zugriff zu eskalieren.

Die folgenden Ressourcentypen können in ihren Erkenntnissen zur Gefährdung ungenutzter Zugriffe kontextuelle Merkmale aufweisen:

- Amazon Elastic Compute Cloud-Instanzen
- AWS Lambda Funktionen
- Dienste von Amazon Elastic Container Service
- Amazon Elastic Kubernetes Service Service-Cluster
- IAM-Benutzer (direkt)

Klassifizierung des Schweregrads

Die Ergebnisse der Exposition werden nach folgenden Kriterien klassifiziert:

- Einfache Entdeckung
- Einfache Ausnutzung
- Wahrscheinlichkeit einer Ausbeutung
- Sensibilisierung der Öffentlichkeit
- Mögliche Auswirkungen
- Primäre Ressourcenkritikalität

Weitere Informationen finden Sie unter Klassifizierung des Schweregrads der Expositionsbefunde.

Vorteile von Expositionsergebnissen

- Weniger manuelle Analysen durch automatisierte Korrelation: Durch automatisierte Korrelation und intelligente Risikopriorisierung wird der Zeit- und Arbeitsaufwand für Sicherheitsanalysen erheblich

reduziert. Security Hub überwacht Ihre AWS Umgebung kontinuierlich und identifiziert und korreliert automatisch Sicherheitsrisiken, die bei manueller Überprüfung möglicherweise übersehen werden.

- Priorisierte Ansicht von Sicherheitsrisiken: Security Hub verwendet ausgeklügelte Algorithmen zur Risikobewertung, um Risiken auf der Grundlage von Schweregrad, Auswirkung, Ressourcenkritikalität und Exploit-Wahrscheinlichkeit zu priorisieren. Auf diese Weise können sich die Sicherheitsteams zunächst auf die wichtigsten Risiken konzentrieren und so die Effizienz der Sicherheitsabläufe verbessern.

Quellen der Feststellungen zur Exposition

Die Ergebnisse zur Exposition beinhalten Daten aus:

- GuardDuty Die Amazon-Integration bietet kontinuierliche Funktionen zur Bedrohungserkennung innerhalb von Risikoergebnissen. Es überwacht böswillige Aktivitäten, potenzielle Kontokompromittierungen und Verhaltensanomalien. Das System bezieht diese Bedrohungserkenntnisse in die umfassendere Risikoanalyse ein und hilft so zu erkennen, wann Bedrohungen zusammen mit anderen Sicherheitsproblemen zu erheblichen Risiken führen.
- Amazon Inspector trägt wichtige Daten zur Schwachstellenbeurteilung zu den Ergebnissen der Exposition bei. Es bietet detaillierte Informationen zur Erreichbarkeit des Netzwerks, zu Softwareschwachstellen und zu Verstößen gegen bewährte Sicherheitsverfahren. Diese Integration hilft zu verstehen, wie Sicherheitslücken über identifizierte Angriffspfade ausgenutzt werden können.
- AWS Security Hub CSPM stellt sicher, dass die Einhaltung von Konfigurationen und Sicherheitsstandards bei der Risikoanalyse berücksichtigt wird. Es bewertet Ressourcen anhand etablierter Sicherheitskontrollen und bewährter Verfahren und bietet so eine Grundlage für das Verständnis konfigurationsbedingter Risiken.
- Amazon Macie verbessert die Ergebnisse von Sicherheitslücken mit Funktionen zur Erkennung und Klassifizierung sensibler Daten. Es identifiziert, wo sich sensible Daten in Ihrer AWS Umgebung befinden, und bewertet potenzielle Datenschutzrisiken, um die potenziellen Auswirkungen identifizierter Sicherheitsrisiken besser zu verstehen.

Bewährte Methoden

- Regelmäßige Überprüfung der Ergebnisse zur Exposition: Ein effektives Expositionsmanagement erfordert strukturierte Überprüfungsprozesse. Organizations sollten tägliche Überprüfungen

kritischer Risiken, wöchentliche Bewertungen des allgemeinen Risikostatus, monatliche Trendanalysen und vierteljährliche Bewertungen der Sicherheitslage durchführen. Dieser mehrstufige Ansatz gewährleistet, dass sowohl unmittelbaren Risiken als auch langfristigen Sicherheitstrends angemessene Aufmerksamkeit geschenkt wird.

- Priorisieren Sie kritische Risiken und Risiken mit hohem Schweregrad: Ein erfolgreiches Risikomanagement hängt von einer effektiven Risikopriorisierung ab. Organizations sollten sich zunächst auf kritische Risiken konzentrieren und dabei die Kritikalität der Ressourcen und die Auswirkungen auf das Geschäft berücksichtigen. Dieser risikobasierte Ansatz trägt dazu bei, dass die Sicherheitsbemühungen mit den Geschäftsprioritäten übereinstimmen und die Risikominderung maximiert wird.
- Implementieren Sie die empfohlenen Abhilfemaßnahmen: Bei der Gefahrenabwehr sollte ein systematischer Ansatz verfolgt werden. Organizations sollten die empfohlenen Abhilfemaßnahmen sorgfältig umsetzen, eine detaillierte Dokumentation der Änderungen führen, gründliche Tests der Änderungen durchführen und die Wirksamkeit der implementierten Korrekturen überprüfen. Dieser methodische Ansatz trägt dazu bei, eine erfolgreiche Risikominderung sicherzustellen und gleichzeitig unbeabsichtigte Folgen zu vermeiden.
- Konfigurieren Sie Regeln für automatisierte Reaktionen: Um den Wert von Risikoergebnissen zu maximieren, ist eine effektive Automatisierung erforderlich. Organizations sollten automatisierte Reaktionsregeln implementieren, entsprechende Benachrichtigungen konfigurieren, effiziente Workflows einrichten und umfassende Prüfpfade führen. Diese Automatisierung trägt dazu bei, eine konsistente und zeitnahe Reaktion auf identifizierte Risiken sicherzustellen und gleichzeitig den manuellen Aufwand zu reduzieren.

Unterstützte Ressourcentypen für Risikopergebnisse in Security Hub

AWS Security Hub generiert Risikopergebnisse für die folgenden AWS Ressourcentypen:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`

- `AWS::S3::Bucket`
- `AWS::SageMaker::NotebookInstance`

Wenn Sie über einen Azure-Connector verfügen, generiert Security Hub auch Risikopergebnisse für die folgenden Arten von Azure-Ressourcen:

- `microsoft.app/containerapps`
- `microsoft.compute/virtualmachines`
- `microsoft.containerservice/managedclusters`
- `microsoft.documentdb/databaseaccounts`
- `microsoft.graph/user`
- `microsoft.sql/servers/databases`
- `microsoft.storage/storageaccounts/blobservices/containers`
- `microsoft.web/sites`

Security Hub generiert einen Risikobefund pro primärer Ressource. Wenn eine Ressource keine oder nur unzureichende Expositionsmerkmale aufweist, generiert Security Hub keine Expositionsfeststellung für diese Ressource.

Unterstützte Merkmalstypen in Security Hub

AWS Security Hub generiert ein Expositionsergebnis, wenn die Ergebnisse der AWS Security Hub CSPM-Kontrolle und Ergebnisse AWS-Services, die von anderen unterstützten Anbietern wie Amazon Inspector generiert wurden, Expositionsmerkmale für eine Ressource enthalten. Die folgende Tabelle enthält Informationen zu den unterstützten Merkmalstypen.

Merkmalstyp	Description	Quelle	Betroffene Ressourcen
Vermutbarkeit	Weist auf eine Ressource mit erteilten Berechtigungen hin AWS Identity and Access Management	Ressource nkonfiguration von AWS Config	AWS Ressource n mit zugehörig en AWS Identity and Access Management Rollen

Merkmalstyp	Description	Quelle	Betroffene Ressourcen
Auswirkung	Gibt den potenziellen Explosionsradius an, wenn die Ressource kompromittiert wird. Er basiert auf den effektiven Berechtigungen der zugehörigen AWS Identity and Access Management Principals, einschließlich der Fähigkeit, Ressourcen zu erstellen und zu ändern, der Wichtigkeit nachgelagerter Ressourcen und der Kritikalität der primären Ressource.	• Effektive Berechtigungsanalyse der zugehörigen Principals. AWS Identity and Access Management • Wichtigkeit der Ressourcen, auf die ein bestimmter AWS Identity and Access Management Auftragger zugreifen kann. Die Kritikalität kann durch Automatisierungsregeln festgelegt werden, oder sie wird anhand des Namens und der Tags der Ressource abgeleitet.	AWS Ressourcen mit zugehörigen Identitäten AWS Identity and Access Management

Merkmalstyp	Description	Quelle	Betroffene Ressourcen
Fehlkonfiguration	Weist auf eine falsch konfigurierte Ressource hin	AWS Security Hub CSPM-Kontrollergebnisse, GuardDuty Amazon-Bedrohungsergebnisse und Informationen zur Ressourcenbestätigung in. AWS Config	Alle Ressourcentypen
Erreichbarkeit	Weist auf offene Netzwerkpfade zu einer Ressource hin	AWS Ergebnisse der Security Hub CSPM-Kontrolle, GuardDuty Amazon-Bedrohungserkenntnisse und Ergebnisse der Amazon Inspector-Netzwerkerreichbarkeit.	Amazon EC2 EC2-Instances, Amazon EKS-Cluster, Lambda-Funktionen und Amazon S3 S3-Buckets
Sensible Daten	Zeigt an, dass eine Ressource vertrauliche Daten enthält	Ergebnisse mit sensiblen Daten	Amazon-S3-Buckets

Merkmalstyp	Description	Quelle	Betroffene Ressourcen
Schwachstelle	Zeigt an, dass eine Ressource eine Schwachstelle aufweist, die von einer Bedrohungsquelle ausgenutzt werden könnte.	Ergebnisse der Sicherheitslücken im Amazon Inspector-Paket und Ergebnisse von GuardDuty Amazon Amazon EC2-Malware.	Amazon EC2 EC2-Instances, Amazon ECS-Services, Amazon EKS-Cluster und Lambda-Funktionen
Kritikalität	Weist auf die Bedeutung einer Ressource für das Unternehmen hin	Wird über Automatisierungsregeln zugewiesen. Wenn die Priorität nicht durch eine Automatisierungsregel festgelegt ist, leitet Security Hub sie aus dem Ressourcennamen und den Tags ab. Weitere Informationen finden Sie unter Ressourcen im Security Hub.	Alle Ressourcentypen

Jedes Merkmal kann mit mehreren Titeln verknüpft werden, die Einzelheiten über die Exposition enthalten, die sich auf die Ressource auswirkt. Beispielsweise könnten Sie in den Details einer EC2-Schwachstelle den Titel Exploit Available für das Merkmal Sicherheitslücke sehen.

Auswirkungen und effektive Genehmigungen

Das Merkmal „Auswirkung“ beschreibt den potenziellen Explosionsradius eines Risikos — also die nachgelagerten Ressourcen, die ein Angreifer erreichen und kompromittieren könnte, wenn die Hauptressource, auf der das Risiko festgestellt wurde, kompromittiert wird. Um die Auswirkungen zu ermitteln, analysiert Security Hub die effektiven Berechtigungen der AWS Identity and Access Management (IAM-) Principals, die der Ressource zugeordnet sind, sowie die Wichtigkeit der Ressourcen.

Effektive Berechtigungen sind die Berechtigungen, über die ein Principal tatsächlich verfügt, nachdem Security Hub seine identitätsbasierten Richtlinien zusammen mit den ressourcenbasierten Richtlinien der Ressourcen, auf die er zugreifen kann, und allen Service Control Policies (SCPs) und Resource Control Policies (RCPs) der AWS Organizations, die für das Konto gelten, bewertet hat. Da effektive Berechtigungen berücksichtigen, was einem Prinzipal gewährt wird, welche Zielressourcen zulassen und welche Richtlinien auf Organisationsebene das Konto einschränken, geben sie die Aktionen, die ein Prinzipal ausführen kann, genauer wider als die identitätsbasierten Richtlinien allein.

Mithilfe effektiver Berechtigungen verfolgt Security Hub die Pfade der Rechteeskalation von der primären Ressource zu anderen Ressourcen in Ihrer Umgebung. Jeder Pfad ist eine Kette von Ressourcen, die durch Berechtigungen miteinander verbunden sind und es einem Angreifer ermöglichen, von einer Ressource zur nächsten zu wechseln. Wenn Security Hub einen konkreten Pfad zu einer vorhandenen Ressource identifiziert, wird dieser Pfad als Teil des Impact-Merkmals angezeigt. Impact berücksichtigt auch Berechtigungen, die über diese Pfade hinausgehen, wie z. B. die Möglichkeit, diese aufzurufen AWS-Services , um andere Ressourcen zu erstellen oder zu ändern, und die Wichtigkeit der primären Ressource. Sie können diese Pfade im Diagramm der potenziellen Angriffspfade überprüfen und Ihren Explosionsradius reduzieren, indem Sie unnötige Berechtigungen entfernen. Weitere Informationen finden Sie unter Gefährdungen in Security Hub mit dem Diagramm des potenziellen Angriffspfads anzeigen.

Generierung von Expositionsergebnissen

Security Hub generiert Erkenntnisse zur Gefährdung nahezu in Echtzeit. Wenn neue Sicherheitserkenntnisse aufgenommen und bestehende Erkenntnisse aktualisiert werden, generiert oder aktualisiert Security Hub die Ergebnisse der Sicherheitslücken nahezu in Echtzeit. Security Hub generiert einen Risikobefund pro Ressourcen-ID.

Security Hub veröffentlicht keine Expositionsergebnisse für Ressourcentypen, die nicht durch Risikopergebnisse gestützt werden. Wenn eine Ressource eine signifikante Anzahl und Kombination

von Merkmalen aufweist, generiert Security Hub einen Risikobefund. Die Anzahl und Kombination der Merkmale bestimmen auch den Schweregrad des Expositionsergebnisses.

Expositionsergebnis der Stichprobe

AWS Security Hub normalisiert die Ergebnisse der Sicherheitslücken im Open Cybersecurity Schema Framework (OCSF).

Beispiel für die Feststellung der Exposition

In der folgenden Stichprobe enthält der `related_events` Parameter Einzelheiten, die sich nur auf den Expositionsergebnis beziehen, wie z. B. die Ergebnisse, die dazu beigetragen haben. Zu den Ergebnissen beitragen die Merkmale und Signale, die mit einem Expositionsergebnis in Verbindung stehen. Ein einzelnes beitragendes Ergebnis kann ein oder mehrere Merkmale umfassen. Der `observables` Parameter identifiziert die Ressource, die dem beitragenden Ergebnis zugeordnet ist. Dies kann sich von dem `resources` Parameter unterscheiden, der die Ressource identifiziert, die mit dem Expositionsergebnis verknüpft ist.


```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
```

```
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
                            "Exploit Available",
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
```

```
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title":  "Lambda function policies should prohibit public access",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
```

```
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "LambdaProdStack"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
LambdaProdStack/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
```

```
    "severity": "Critical",
    "severity_id": 5,
    "impact": "High",
    "impact_id": 3,
    "likelihood": "Very High",
    "likelihood_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
    }
}
```

Bestimmung des Schweregrads eines Expositionsergebnisses

AWS Security Hub weist jedem Sicherheitsrisiko, das entdeckt wird, einen Standardschweregrad von`CRITICAL`, `HIGHMEDIUM`, oder `LOW` zu. Expositionsergebnisse mit einem Schweregrad von `INFORMATIONAL` werden nicht veröffentlicht. Security Hub bestimmt den Schweregrad einer Risikofeststellung, indem es zwei Dimensionen, Wahrscheinlichkeit und Auswirkung, in einer Risikomatrix kombiniert. Die Wahrscheinlichkeit gibt an, wie leicht das Risiko ausgenutzt werden kann, und die Wirkung spiegelt das Ausmaß des Schadens wider, wenn es ausgenutzt wird.

In Fällen, in denen die Auswirkungen für eine Ressource nicht bestimmt werden können, basiert der Schweregrad ausschließlich auf der Wahrscheinlichkeit.

Risikomatrix

Die folgende Tabelle zeigt, wie Wahrscheinlichkeit und Auswirkung zusammen den endgültigen Schweregrad eines Expositionsergebnisses ergeben. Mit der Wahrscheinlichkeit wird ein Ausgangsschweregrad festgelegt, und die Wirkung passt ihn an: Bei starker Wirkung wird der Schweregrad um eine Stufe erhöht (begrenzt auf`CRITICAL`), bei mittlerer Wirkung bleibt der Schweregrad unverändert, und bei geringer Wirkung wird der Schweregrad um eine Stufe verringert (Untergrenze bei). `INFORMATIONAL` Bei der Auswirkung wird nur der Schweregrad angepasst, der sich aus der Wahrscheinlichkeit ergibt. Die Wirkung allein führt noch nicht zu einem Expositionsergebnis.

Risikomatrix zum Schweregrad

Wahrscheinlichkeit ↓/Auswirkung →	Niedrig	Medium	Hoch
Sehr hoch	HIGH (HOCH)	KRITISCH	KRITISCH
Hoch	MITTEL	HIGH (HOCH)	KRITISCH
Mittel	NIEDRIG	MITTEL	HIGH (HOCH)
Niedrig	INFORMATIV	NIEDRIG	MITTEL

> **Note**
>
> Eine geringe Wahrscheinlichkeit in Kombination mit geringen Auswirkungen führt zu einem Schweregrad von`INFORMATIONAL`. Security Hub veröffentlicht keine Risikoergebnisse mit diesem Schweregrad, sodass sie nicht auf der Seite Risiken oder in den GetFindingsV2Ergebnissen erscheinen.

Wahrscheinlichkeit

Die Wahrscheinlichkeit gibt an, wie leicht ein Risiko ausgenutzt werden kann, und zwar auf der Grundlage der jeweiligen Merkmale der Ressource, wie Vermutbarkeit, Fehlkonfiguration, Erreichbarkeit, sensible Daten und Sicherheitslücke. Security Hub verwendet verschiedene Merkmale, um die Wahrscheinlichkeit zu beurteilen, darunter die folgenden:

- Bekanntheit — Das Ausmaß, in dem die Gefahr nicht theoretisch ist, sondern es sich um öffentlich zugängliche oder automatisierte Exploits handelt.
- Einfache Erkennung — ob automatisierte Tools wie ein Port-Scan oder eine Internetsuche zur Verfügung stehen, um die gefährdete Ressource zu entdecken.
- Einfache Ausnutzung — Die Leichtigkeit, mit der ein Bedrohungsakteur die Gefahr ausnutzen kann. Wenn beispielsweise offene Netzwerkpfade oder falsch konfigurierte Metadaten existieren, kann ein Bedrohungsakteur die Gefahr leichter ausnutzen.
- Wahrscheinlichkeit eines Exploits — Die Wahrscheinlichkeit, dass das Sicherheitsrisiko in den nächsten 30 Tagen ausgenutzt wird. Dieser Faktor entspricht dem Exploit Prediction Scoring System (EPSS).

Auswirkung

Die Wirkung misst das Ausmaß der Schädigung Ihrer Umwelt, wenn die Exposition ausgenutzt wird. Eine Gefährdung könnte beispielsweise zum Verlust der Rechenschaftspflicht, zum Verlust der Verfügbarkeit, zum Verlust der Vertraulichkeit aufgrund von Datenverlust oder zum Verlust der Integrität aufgrund von Datenbeschädigung führen.

Um die Auswirkungen zu beurteilen, analysiert Security Hub die effektiven Berechtigungen der mit der Ressource AWS Identity and Access Management verknüpften Principals, um zu ermitteln, welche Aktionen AWS-Services ein Angreifer ausführen könnte. Es identifiziert auch die vorhandenen Ressourcen, auf die ein Angreifer durch Rechteausweitung zugreifen und diese gefährden könnte. Weitere Informationen finden Sie unter Auswirkungen und effektive Genehmigungen.

Überprüfung der Ergebnisse zur Exposition

Sie können alle Ihre Erkenntnisse zur Gefährdung in der Security Hub Hub-Konsole und mit der GetFindingsV2API überprüfen. Auf der Seite Exposures in der Security Hub Hub-Konsole werden alle aktiven Risikoergebnisse angezeigt. Die Ergebnisse der Exposition werden nach abnehmendem Schweregrad aufgelistet. Sie können Ihre Expositionsergebnisse filtern, indem Sie Filter mit der Suchleiste Filter hinzufügen oder entfernen. Sie können Ihre Expositionsergebnisse mit der Dropdownliste Gruppieren nach gruppieren. Sie können Ihre Expositionsergebnisse auch mit dem Schnellfilter-Menü filtern.

Einzelheiten zu den Expositionsergebnissen

Sie können sich viele Details zu einem Expositionsergebnis ansehen. Diese Details sind in der Security Hub Hub-Konsole auf mehrere Tabs aufgeteilt. Auf der Registerkarte „Übersicht“ finden Sie wichtige Informationen zur Risikofeststellung. Auf der Registerkarte Merkmale sind die Merkmale und Signale aufgeführt, die mit einem Expositionsergebnis verknüpft sind. Die Registerkarte Ressourcen enthält Details zu den Ressourcen und Ressourcen-Tags, die mit einem Expositionsergebnis verknüpft sind. Die folgende Liste enthält Beschreibungen der Einzelheiten zu den Ergebnissen der Exposition.

- Titel des Befundes — Der Titel des Expositionsergebnisses.
- Schweregrad — Der Schweregrad des Expositionsergebnisses. Security Hub verwendet die Anzahl und Kombination von Merkmalen für eine Ressource, um den Schweregrad einer Risikofeststellung zu bestimmen. Der Schweregrad kann`CRITICAL`, `HIGHMEDIUM`, oder sein`LOW`. Security Hub veröffentlicht keine Risikopergebnisse mit einem Schweregrad von`INFORMATIONAL`. Sie können

das `Severity` über die Security Hub Hub-Konsole oder mit dem BatchUpdateFindingsV2API-Vorgang aktualisieren.

- Beschreibung — Die Beschreibung des Expositionsergebnisses.
- Typ — Der Name des Typs der Risikoermittlung. Der Name könnte beispielsweise wie folgt aussehen`Exposure/Potential Impact/Resource Hijacking`.
- Konto — Die ID des Unternehmens AWS-Konto , in dem der Risikoergebnis generiert wurde.
- Alter — Gibt an, wie lange der Expositionsergebnis aktiv ist.
- Erstellungszeit — Ein Zeitstempel, der angibt, wann der Expositionsergebnis erstellt wurde.
- Änderungszeit — Ein Zeitstempel, der angibt, wann das Expositionsergebnis zuletzt aktualisiert wurde.
- Region — Der AWS-Region Ort, an dem der Expositionsergebnis generiert wurde.
- Produktname — Der Name des Produkts, das zur Expositionsermittlung geführt hat. Dies wird immer Security Hub Exposure Detection sein.
- Firmenname — Der Name des Unternehmens, das die Risikofeststellung generiert hat. Das wird immer so sein AWS.
- Name der Aktivität — Der Name der Aktivität, die zuletzt anhand des Ergebnisses ausgeführt wurde.
- Status — Der Status dieser Expositionsfeststellung.
- Fund-ID — Eine eindeutige Kennung, die mit dem Expositionsergebnis verknüpft ist.
- Potenzieller Angriffspfad (nur Konsole) — Eine interaktive Visualisierung, die zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und die Kontrolle über diese übernehmen können, die mit einem Sicherheitsrisiko verbunden sind. Weitere Informationen finden Sie unter Gefährdungen in Security Hub mit dem Diagramm des potenziellen Angriffspfads anzeigen.
- Merkmale — Identifiziert Merkmalstypen und Merkmalstitel, die mit dem Expositionsergebnis verknüpft sind. In der Security Hub Hub-Konsole können Sie Eigenschaften nach Merkmalstyp oder Signal anzeigen. Auf diese Weise können Sie wichtige Ergebnisse im Zusammenhang mit der jeweiligen Exposition analysieren.
- Sanierung — Links zu Unterlagen zur Problembehebung, die sich auf die bei der Exposition identifizierten Merkmale beziehen.
- Ressourcen — Identifiziert die Ressource, die mit dem Expositionsergebnis verknüpft ist.

Überprüfung der Einzelheiten der Expositionsergebnisse

In diesem Thema wird beschrieben, wie Sie Details zu Risikoergebnissen in der AWS Security Hub Hub-Konsole und mit der API überprüfen können.

Details zu einer Risikofeststellung in der Security Hub Hub-Konsole überprüfen

So zeigen Sie Details zu einer Risikofeststellung in der Security Hub Hub-Konsole an

1. Melden Sie sich mit Ihren Anmeldeinformationen an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich die Option Exposures aus.
3. Wählen Sie ein Risikoergebnis aus, dessen Details Sie anzeigen möchten.

Überprüfen Sie die Details zu einem Risikoergebnis mit der API

Sie können die Ergebnisse zur Exposition mit der GetFindingsV2API oder mit der überprüfen AWS CLI. Sie können alle Expositionsergebnisse anhand des `metadata.product.feature.uid` Felds mit dem `security-hub/Exposure` Wert filtern. Weitere Informationen finden Sie unter GetFindingsV2.

Beispielbefehl

Im Folgenden finden Sie ein AWS CLI Beispiel, mit dem die 10 zuletzt generierten Expositionsergebnisse in Ihrem Konto abgerufen werden. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
aws securityhub get-findings-v2 \
--max-results '10' \
--filter '{"CompositeFilters": [{"StringFilters":
 [{"FieldName":"metadata.product.feature.uid","Filter": {"Value":"security-hub/
Exposure","Comparison":"EQUALS"}} ]}]}'
```

Gefährdungen in Security Hub mit dem Diagramm des potenziellen Angriffspfads anzeigen

Das Diagramm des potenziellen Angriffspfads ist eine interaktive Visualisierung, die zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und die Kontrolle darüber übernehmen können, die

mit einer Sicherheitslücke verbunden sind. Sie können auf dieses Diagramm nur in der Security Hub Hub-Konsole von der Seite Exposures aus zugreifen. Wenn Sie sich Details zu einem gefundenen Sicherheitsrisiko ansehen, enthält die Registerkarte „Übersicht“ einen Abschnitt mit den Bezeichnungen „Potenzieller Angriffspfad“ und „Explosionsradius“.

Das Diagramm des Angriffspfads zeigt die primäre Ressource, über die das Risiko generiert wurde, den Netzwerkpfad (falls zutreffend) und die nachgelagerten Ressourcen, auf die ein Angreifer durch die Eskalation von Berechtigungen zugreifen könnte. Wenn Security Hub konkrete Pfade zur Rechteerweiterung von der primären Ressource zu anderen Ressourcen in Ihrer Umgebung identifiziert, werden diese als Explosionsradius-Teil des Diagramms angezeigt. Jeder Knoten steht für eine Ressource, und die Verbindungen zwischen den Knoten zeigen die Berechtigungen, die es einem Angreifer ermöglichen, von einer Ressource zur nächsten zu wechseln.

In diesem Abschnitt der Registerkarte „Übersicht“ können Sie AWS Ressourcen auswählen und in das Diagramm mit dem potenziellen Angriffspfad verschieben. Mit den Symbolen zum Vergrößern und Verkleinern können Sie sich auf bestimmte Bereiche des Diagramms mit dem Angriffspfad konzentrieren. Sie können das Diagramm des Angriffspfads im Vollbildmodus und aus dem Vollbildmodus mithilfe des Vollbildsymbols erweitern. Die Legende gibt die Primärressource, die beteiligten Ressourcen, die Ressourcen im Explosionsradius und die Anzahl der beitragenden Eigenschaften farblich an und zeigt die Merkmalskategorien und die Anzahl der Eigenschaften im Diagramm des Angriffspfads. Sie können Details zu einer Ressource anzeigen, indem Sie eine Ressource auswählen und dann Ressourcendetails anzeigen wählen. Sie können auch die mit einer Ressource verknüpfte ID und AWS-Konto Nummer kopieren. Offenlegungsergebnisse mit einem Erreichbarkeitsmerkmal zeigen das öffentliche Internet und den zusammengebrochenen Netzwerkpfad im Diagramm des Angriffspfads. Sie können sich dieses Detail ansehen, indem Sie den Knoten mit dem ausgeblendeten Netzwerkpfad auswählen.

Wählen Sie die Registerkarte Folgenabschätzung, um die nachgelagerten Ressourcen und die Wege zur Rechteerweiterung, die sie miteinander verbinden, einzusehen. Jeder Pfad zeigt die Ressourcenkette, die ein Angreifer durchqueren könnte, und die spezifischen Berechtigungen für jeden Schritt. Weitere Informationen zu Wirkungsmerkmalen und effektiven Berechtigungen finden Sie unterAuswirkungen und effektive Genehmigungen.

Behebung von Expositionsfeststellungen

In den Themen dieses Abschnitts werden Maßnahmen zur Behebung von Expositionsergebnissen in verschiedenen Bereichen beschrieben. AWS-Services

Das `Remediation` Feld des OCSF-Formats enthält zwei Felder: `remediation` und. `references`

```
"Remediation": {
    "Recommendation": {
        "remediation":{"desc":"String",
        "references":["string array"]}
    }
},
```

> **Note**
>
> Die in den folgenden Abschnitten enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen AWS Ressourcen.

Korrigieren von Risiken für DynamoDB-Tabellen

AWS Security Hub kann Risikoprüfungen für DynamoDB-Tabellen generieren.

Auf der Security Hub-Konsole werden die DynamoDB-Tabelle, die an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der Security Hub GetFindingsV2 CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema enthaltenen Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Ressourcen. AWS

Inhalt

- Merkmale einer Fehlkonfiguration in DynamoDB
  - Für die DynamoDB-Tabelle ist die Point-in-Time-Wiederherstellung deaktiviert
  - Die DynamoDB-Tabelle ist nicht durch einen Backup-Plan abgedeckt
  - Für die DynamoDB-Tabelle ist der Löschschutz deaktiviert

Merkmale einer Fehlkonfiguration in DynamoDB

Im Folgenden werden die Merkmale der Fehlkonfiguration und die Schritte zur Behebung von DynamoDB-Tabellen beschrieben.

Für die DynamoDB-Tabelle ist die Point-in-Time-Wiederherstellung deaktiviert

Problembehebung: Aktivieren Sie DynamoDB Point-in-Time-Recovery

DynamoDB Point-in-Time Recovery bietet kontinuierliche automatische Backups für Ihre DynamoDB-Tabellendaten. Informationen zur Wiederherstellung einer DynamoDB-Tabelle zu einem bestimmten Zeitpunkt finden Sie unter Wiederherstellen einer DynamoDB-Tabelle zu einem bestimmten Zeitpunkt im Amazon DynamoDB-Entwicklerhandbuch.

Die DynamoDB-Tabelle ist nicht durch einen Backup-Plan abgedeckt

AWS Backup bietet einen zentralisierten Dienst zur Konfiguration, Verwaltung und Automatisierung von Backups für alle AWS Dienste, einschließlich DynamoDB. Ohne einen Backup-Plan fehlen Ihrer Tabelle geplante, automatische Backups mit anpassbaren Aufbewahrungsfristen, was zu erheblichen Sicherheitsrisiken führt. Ein Angreifer könnte Ihre Tabellendaten in böswilliger Absicht beschädigen oder löschen. Ohne ordnungsgemäße Backups haben Sie möglicherweise keine Wiederherstellungsoption außerhalb des Point-in-Time Wiederherstellungsfensters (falls aktiviert), was möglicherweise zu einem dauerhaften Datenverlust führen kann. Schützen Sie Ihre DynamoDB-Tabellen mit einem Backup-Plan, indem Sie den bewährten Methoden zum Datenschutz folgen.

Problembehebung: Erstellen Sie einen Backup-Plan

Bevor Sie einen Backup-Plan erstellen, legen Sie eine angemessene Sicherungshäufigkeit und Aufbewahrungsfristen für Ihre Daten fest. Informationen zur Erstellung eines Backup-Plans finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Developer Guide.

Für die DynamoDB-Tabelle ist der Löschschutz deaktiviert

Der Löschschutz verhindert das versehentliche Löschen von DynamoDB-Tabellen. Wenn der Löschschutz deaktiviert ist, sind DynamoDB-Tabellen anfällig für unbeabsichtigtes Löschen durch Konsolenaktionen, API-Aufrufe, CLI-Befehle oder automatisierte Prozesse. Dadurch kann Ihre AWS Umgebung einem Datenverlust ausgesetzt sein, da eine nicht autorisierte Entität mit Zugriff auf Ihre AWS Umgebung absichtlich Tabellen löschen könnte, was zu Betriebsunterbrechungen und dauerhaftem Datenverlust führen könnte. Aktivieren Sie den Datenschutz für DynamoDB-Tabellen gemäß den bewährten Datenschutzpraktiken.

Behebung: Aktivieren Sie den Löschschutz

Wenn Sie mehrere Tabellen verwalten, sollten Sie erwägen, CloudFormation die Tabelleneigenschaften in großen Mengen zu aktualisieren. Sie können Ihre CloudFormation Vorlagen so ändern, dass sie `DeletionProtectionEnabled` Eigenschaften enthalten, und Ihre Stapel aktualisieren. Vergewissern Sie sich nach Abschluss der Korrektur, dass der Löschschutz in der Dropdownliste Zusätzliche Informationen in der Tabelle „Einstellungen“ aktiviert ist.

Behebung von Risiken für EC2-Instances

AWS Security Hub kann Risikopergebnisse für Amazon Elastic Compute Cloud (EC2) -Instances generieren.

Auf der Security Hub Hub-Konsole sind die EC2-Instance, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

> **Note**
>
> Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- Merkmale der Fehlkonfiguration für EC2-Instances
  - Die EC2-Instance ermöglicht den Zugriff auf IMDS mit Version 1
  - Die Amazon EC2 EC2-Instance verfügt über eine Sicherheitsgruppe oder Netzwerk-ACL, die SSH- oder RDP-Zugriff ermöglicht.
  - Die Amazon EC2 EC2-Instance hat eine offene Sicherheitsgruppe
- Erreichbarkeitsmerkmale für EC2-Instances
  - Die EC2-Instance ist über das Internet erreichbar
- Merkmale der Sicherheitslücke für EC2-Instances
  - Die EC2-Instance weist Software-Sicherheitslücken auf, die im Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist
  - Die Amazon EC2 EC2-Instance weist Softwareschwachstellen auf
  - Die EC2-Instance hat ein Betriebssystem End-Of-Life
  - Die EC2-Instance enthält schädliche Softwarepakete
  - Die EC2-Instance enthält schädliche Dateien
- Auswirkungsmerkmale für EC2-Instances
  - Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff
  - Hat einen direkten politischen Eskalationspfad
  - Hat einen Hijack-Pfad für Vertrauensrichtlinien
  - Hat einen Pfad zur Daten-Ransomware
  - Hat den Beschränkungspfad entfernt
  - Hat die Rolle bestanden, den Executor-Pfad erstellen
  - Hat den Executor-Pfad für die Swap-Rolle bereits
  - Hat einen Eskalationspfad für die Rollenkette
  - Hat einen privilegierten Executor-Pfad für Inject-Code
  - Hat den Audit-Trail-Pfad deaktiviert

- Hat Zugriff auf den vorhandenen Executor-Pfad
- Hat einen Pfad zum Minting von Anmeldeinformationen
- Hat den Datenzugriffspfad bestanden
- Hat den Pfad zur Übernahme der Rolle, der Aufgabe
- Hat einen Single-Hop-Datenzugriffspfad
- Hat einen Pfad zur Weiterentwicklung der Fähigkeiten
- Geschäftliche Kritikalität

Merkmale der Fehlkonfiguration für EC2-Instances

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für EC2-Instances und empfohlene Schritte zur Behebung.

Die EC2-Instance ermöglicht den Zugriff auf IMDS mit Version 1

Instance-Metadaten sind Daten über Ihre Amazon EC2 EC2-Instance, die Anwendungen zur Konfiguration oder Verwaltung der laufenden Instance verwenden können. Der Instance-Metadatenservice (IMDS) ist eine On-Instance-Komponente, die von Code auf der Instance verwendet wird, um sicher auf Instance-Metadaten zuzugreifen. Wenn IMDS nicht ordnungsgemäß gesichert ist, kann es zu einem potenziellen Angriffsvektor werden, da es Zugriff auf temporäre Anmeldeinformationen und andere sensible Konfigurationsdaten bietet. IMDSv2 bietet einen besseren Schutz vor Ausnutzung durch sitzungsorientierte Authentifizierung, die ein Sitzungstoken für Metadatenanfragen erfordert und die Sitzungsdauer begrenzt. Konfigurieren Sie Amazon EC2 EC2-Instances gemäß den Standardsicherheitsprinzipien für die Verwendung von IMDSv2 und deaktivieren Sie IMDSv1.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Testen Sie die Anwendungskompatibilität

Bevor Sie IMDSv2 implementieren, testen Sie Ihre Instance, um sicherzustellen, dass sie mit IMDSv2 kompatibel ist. Einige Anwendungen oder Skripte benötigen möglicherweise IMDSv1 für die Kernfunktionalität und erfordern eine zusätzliche Konfiguration. Weitere Informationen zu Tools und empfohlenen Pfaden zum Testen der Anwendungskompatibilität finden Sie unter Übergang zur Verwendung von Instance Metadata Service Version 2 im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Aktualisieren Sie die Instanz, um IMDSv2 zu verwenden

Ändern Sie bestehende Instanzen, um IMDSv2 zu verwenden. Weitere Informationen finden Sie unter Ändern von Instance-Metadaten-Optionen für bestehende Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Updates auf Instances in einer Auto Scaling Scaling-Gruppe anwenden

Wenn Ihre Instance Teil einer Auto Scaling Scaling-Gruppe ist, aktualisieren Sie Ihre Startvorlage oder Startkonfiguration mit einer neuen Konfiguration und führen Sie eine Instance-Aktualisierung durch.

Die Amazon EC2 EC2-Instance verfügt über eine Sicherheitsgruppe oder Netzwerk-ACL, die SSH- oder RDP-Zugriff ermöglicht.

Fernzugriffsprotokolle wie SSH und RDP ermöglichen es Benutzern, von externen Standorten aus eine Verbindung zu Amazon EC2 EC2-Instances herzustellen und diese zu verwalten. Wenn Sicherheitsgruppen uneingeschränkten Zugriff auf diese Protokolle aus dem Internet zulassen, vergrößern sie die Angriffsfläche Ihrer Amazon EC2 EC2-Instances, indem sie den Internetzugang auf Ihre Instance ermöglichen. Beschränken Sie den Fernzugriff gemäß den Standardsicherheitsprinzipien auf bestimmte, vertrauenswürdige IP-Adressen oder Bereiche.

Behebung: Ändern Sie die Regeln für Sicherheitsgruppen

Beschränken Sie den Zugriff auf Ihre Amazon EC2 EC2-Instances auf bestimmte vertrauenswürdige IP-Adressen. Beschränken Sie den SSH- und RDP-Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder verwenden Sie die CIDR-Notation, um IP-Bereiche anzugeben (z. B. 192.168.1). 0/24). Informationen zum Ändern von Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Die Amazon EC2 EC2-Instance hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Amazon EC2 EC2-Instances, um den eingehenden und ausgehenden Datenverkehr zu kontrollieren. Offene Sicherheitsgruppen, die uneingeschränkten Zugriff von jeder IP-Adresse aus ermöglichen, können Ihre Instances unbefugten Zugriffen aussetzen. Halten Sie sich an die Standardsicherheitsprinzipien und beschränken Sie den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen Sie die Sicherheitsgruppenregeln und bewerten Sie die aktuelle Konfiguration

Prüfen Sie, welche Ports offen und von weiten IP-Bereichen aus zugänglich sind, z. `(0.0.0.0/0 or ::/0)` B. Anweisungen zum Anzeigen von Sicherheitsgruppendetails finden Sie DescribeSecurityGroupsin der API-Referenz zum Porting Assistant for .NET.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken. Informationen zum Ändern von Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon EC2 EC2-Benutzerhandbuch.

Erreichbarkeitsmerkmale für EC2-Instances

Hier finden Sie Merkmale der Erreichbarkeit für EC2-Instances und empfohlene Schritte zur Problembehebung.

Die EC2-Instance ist über das Internet erreichbar

Amazon EC2 EC2-Instances mit Ports, die über das Internet erreichbar sind, können Ihre Instance offenlegen. Die Erreichbarkeit kann über ein Internet-Gateway (einschließlich Instances hinter Application Load Balancers oder Classic Load Balancers), eine VPC-Peering-Verbindung oder ein virtuelles VPN-Gateway erfolgen. Halten Sie sich an die Standardsicherheitsprinzipien und implementieren Sie Netzwerkzugriffskontrollen mit geringsten Rechten, indem Sie den eingehenden Datenverkehr auf die erforderlichen Quellen und Ports beschränken.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Ändern oder entfernen Sie Sicherheitsgruppenregeln

Öffnen Sie auf der Registerkarte Ressourcen die Ressource für die Amazon EC2-Sicherheitsgruppe. Prüfen Sie, ob ein Internetzugang erforderlich ist, damit die Instance funktioniert. Ändern oder

entfernen Sie Sicherheitsgruppenregeln für eingehenden Datenverkehr, die uneingeschränkten Zugriff ermöglichen (`0.0.0.0/0`oder`::/0`). Implementieren Sie restriktivere Regeln, die auf bestimmten IP-Bereichen oder Sicherheitsgruppen basieren. Wenn ein eingeschränkter öffentlicher Zugriff erforderlich ist, beschränken Sie den Zugriff auf bestimmte Ports und Protokolle, die für die Funktion der Instanz erforderlich sind. Anweisungen zur Verwaltung von Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon EC2 EC2-Benutzerhandbuch.

Netzwerk-ACLs aktualisieren

Überprüfen und ändern Sie die Netzwerkzugriffskontrolllisten (ACLs), die dem Subnetz der Instance zugeordnet sind. Stellen Sie sicher, dass die ACL-Einstellungen mit den Änderungen der Sicherheitsgruppe übereinstimmen und nicht unbeabsichtigt öffentlichen Zugriff zulassen. Anweisungen zum Ändern von Netzwerk-ACLs finden Sie unter Arbeiten mit Netzwerk-ACLs im Amazon VPC-Benutzerhandbuch.

Alternative Zugriffsmethoden

Erwägen Sie die folgenden Optionen für alternative Zugriffsmethoden:

- Verwenden Sie das NAT-Gateway für ausgehende Internetkonnektivität — Für Instances in privaten Subnetzen, die Zugriff auf das Internet benötigen (z. B. um Updates herunterzuladen), sollten Sie ein NAT-Gateway verwenden, anstatt eine öffentliche IP-Adresse zuzuweisen. Ein NAT-Gateway ermöglicht es Instances in privaten Subnetzen, ausgehende Verbindungen zum Internet zu initiieren und gleichzeitig eingehende Verbindungen aus dem Internet zu verhindern.
- Verwenden Sie Systems Manager Session Manager — Session Manager bietet sicheren Shell-Zugriff auf Ihre Amazon EC2 EC2-Instances, ohne dass eingehende Ports erforderlich sind, SSH-Schlüssel verwaltet oder Bastion-Hosts verwaltet werden müssen.
- Verwenden Sie WAF und Elastic Load Balancing oder Application Load Balancer — Für Instances, auf denen Webanwendungen ausgeführt werden, sollten Sie erwägen, einen LB in Kombination mit einer AWS Web Application Firewall (WAF) zu verwenden. LBs können so konfiguriert werden, dass Ihre Instances in privaten Subnetzen ausgeführt werden können, während der LB in einem öffentlichen Subnetz läuft und den Internetverkehr abwickelt. Das Hinzufügen einer WAF zu Ihrem Load Balancer bietet zusätzlichen Schutz vor Web-Exploits und Bots.

Merkmale der Sicherheitslücke für EC2-Instances

Im Folgenden finden Sie die Merkmale der Sicherheitslücken für EC2-Instances und empfohlene Schritte zur Behebung.

Die EC2-Instance weist Software-Sicherheitslücken auf, die im Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist

Softwarepakete, die auf EC2-Instances installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Kritische CVEs stellen erhebliche Sicherheitsrisiken für Ihre Umgebung dar. AWS Unbefugte Principals können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Wahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Patchen Sie diese Sicherheitslücken, um Ihre Instanz zu schützen.

Behebung: Aktualisieren Sie die betroffenen Instanzen

Sehen Sie sich den Abschnitt „Referenzen“ auf der Registerkarte „Sicherheitslücke“ des Merkmals an. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Folgen Sie den entsprechenden Abhilfemaßnahmen anhand dieser allgemeinen Richtlinien:

Verwenden Sie Systems Manager Patch Manager, um Patches für Betriebssysteme und Anwendungen anzuwenden. Patch Manager unterstützt Sie bei der automatischen Auswahl und Bereitstellung von Betriebssystem- und Softwarepatches für große Gruppen von Instanzen. Wenn Sie Patch Manager nicht konfiguriert haben, aktualisieren Sie das Betriebssystem auf jeder betroffenen Instanz manuell.

Aktualisieren Sie die betroffenen Anwendungen gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. Um Anwendungsupdates über mehrere Instanzen hinweg zu verwalten, sollten Sie den Systems Manager State Manager verwenden, um Ihre Software in einem konsistenten Zustand zu halten. Wenn keine Updates verfügbar sind, sollten Sie erwägen, die anfällige Anwendung zu entfernen oder zu deaktivieren, bis ein Patch veröffentlicht wird, oder Sie sollten andere Abhilfemaßnahmen ergreifen, z. B. den Netzwerkzugriff auf die Anwendung einschränken oder anfällige Funktionen deaktivieren.

Folgen Sie den spezifischen Empfehlungen zur Problembehebung im Ergebnis von Amazon Inspector. Dies kann das Ändern von Sicherheitsgruppenregeln, das Ändern von Instance-Konfigurationen oder das Anpassen von Anwendungseinstellungen beinhalten.

Prüfen Sie, ob die Instance Teil der Auto Scaling Group ist. AMI-replacement Das Patchen erfolgt auf unveränderlichen Infrastrukturen, indem die AMI-ID aktualisiert wird, die für die Bereitstellung neuer Amazon EC2 EC2-Instances in einer Auto Scaling Scaling-Gruppe konfiguriert ist. Wenn Sie

ein custom/golden AMI verwenden, erstellen Sie eine Instance mit dem neuen AMI, passen Sie dann die Instance an und erstellen Sie ein neues goldenes AMI. Weitere Informationen finden Sie unter Patchen von AMI-Updates (Verwenden von gepatchten AMIs für Auto Scaling Scaling-Gruppen).

Überlegungen für die Zukunft

Um future Vorkommnisse zu verhindern, sollten Sie die Implementierung eines Vulnerability Management-Programms in Betracht ziehen. Amazon Inspector kann so konfiguriert werden, dass auf Ihren Instances automatisch nach CVEs gesucht wird. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Instanzen so gering wie möglich zu halten.

Die Amazon EC2 EC2-Instance weist Softwareschwachstellen auf

Softwarepakete, die auf Amazon EC2 EC2-Instances installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Nicht kritische CVEs stellen Sicherheitslücken dar, die im Vergleich zu kritischen CVEs einen geringeren Schweregrad oder eine geringere Ausnutzbarkeit aufweisen. Diese Sicherheitslücken stellen zwar ein geringeres unmittelbares Risiko dar, aber Angreifer können diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Folgen Sie den bewährten Sicherheitsmethoden und patchen Sie diese Sicherheitslücken, um Ihre Instance vor Angriffen zu schützen.

Behebung: Aktualisieren Sie die betroffenen Instanzen

Verwenden Sie AWS Systems Manager Patch Manager, um Patches für Betriebssysteme anzuwenden. Patch Manager unterstützt Sie bei der automatischen Auswahl und Bereitstellung von Betriebssystem- und Softwarepatches für große Gruppen von Instanzen. Wenn Sie Patch Manager nicht konfiguriert haben, aktualisieren Sie das Betriebssystem auf jeder betroffenen Instanz manuell.

Aktualisieren Sie die betroffenen Anwendungen gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. Um Anwendungsupdates über mehrere Instanzen hinweg zu verwalten, sollten Sie den AWS Systems Manager State Manager verwenden, um Ihre Software in einem konsistenten Zustand zu halten. Wenn keine Updates verfügbar sind, sollten Sie erwägen, die anfällige Anwendung zu entfernen oder zu deaktivieren, bis ein Patch veröffentlicht wird, oder Sie sollten andere Abhilfemaßnahmen ergreifen, z. B. den Netzwerkzugriff auf die Anwendung einschränken oder anfällige Funktionen deaktivieren.

Folgen Sie den spezifischen Empfehlungen zur Problembehebung im Ergebnis von Amazon Inspector. Dies kann das Ändern von Sicherheitsgruppenregeln, das Ändern von Instance-Konfigurationen oder das Anpassen der Anwendungseinstellungen beinhalten.

Prüfen Sie, ob die Instance Teil der Auto Scaling Group ist. AMI-replacement Das Patchen erfolgt auf unveränderlichen Infrastrukturen, indem die AMI-ID aktualisiert wird, die für die Bereitstellung neuer Amazon EC2 EC2-Instances in einer Auto Scaling Scaling-Gruppe konfiguriert ist. Wenn Sie ein custom/golden AMI verwenden, erstellen Sie eine Instance mit dem neuen AMI, passen Sie dann die Instance an und erstellen Sie ein neues goldenes AMI. Weitere Informationen finden Sie unter Patchen von AMI-Updates (Verwenden von gepatchten AMIs für Auto Scaling Scaling-Gruppen).

Überlegungen für die Zukunft

Um future Vorkommnisse zu verhindern, sollten Sie die Implementierung eines Vulnerability Management-Programms in Betracht ziehen. Amazon Inspector kann so konfiguriert werden, dass auf Ihren Instances automatisch nach CVEs gesucht wird. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Instanzen so gering wie möglich zu halten.

Die EC2-Instance hat ein Betriebssystem End-Of-Life

Auf der EC2-Instance wird ein auslaufendes Betriebssystem ausgeführt, das vom ursprünglichen Entwickler nicht mehr unterstützt oder verwaltet wird. Dadurch ist die Instance Sicherheitslücken und potenziellen Angriffen ausgesetzt. Wenn Betriebssysteme das Ende ihrer Lebensdauer erreichen, stellen die Anbieter in der Regel die Veröffentlichung neuer Sicherheitsempfehlungen ein. Bestehende Sicherheitsempfehlungen können auch aus den Feeds der Anbieter entfernt werden. Infolgedessen könnte Amazon Inspector möglicherweise aufhören, Ergebnisse für bekannte CVEs zu generieren, was zu weiteren Sicherheitslücken führen würde.

Informationen zu Betriebssystemen, deren Lebensdauer abgelaufen ist und die von Amazon Inspector erkannt werden können, finden Sie im Amazon Inspector Inspector-Benutzerhandbuch unter Nicht mehr erhältliche Betriebssysteme.

Behebung: Update auf eine unterstützte Betriebssystemversion

Aktualisieren Sie auf eine unterstützte Version des Betriebssystems. Öffnen Sie im Expositionsnachweis die Ressource, um auf die betroffene Ressource zuzugreifen. Bevor Sie die Betriebssystemversion auf Ihrer Instance aktualisieren, erstellen Sie einen Snapshot oder ein AMI-Backup für den Fall, dass Sie ein Rollback durchführen müssen. Eine Liste der derzeit unterstützten

Betriebssystemversionen finden Sie anschließend unter Unterstützte Betriebssysteme im Amazon Inspector Inspector-Benutzerhandbuch.

Die EC2-Instance enthält schädliche Softwarepakete

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihre Instanz dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Entfernen Sie bösartige Pakete gemäß den bewährten Sicherheitsmethoden, um Ihre Instance vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie bösartige Pakete

Sehen Sie sich die Informationen zu den bösartigen Paketen im Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des jeweiligen Merkmals an, um mehr über die Bedrohung zu erfahren. Entfernen Sie die identifizierten bösartigen Pakete mit dem entsprechenden Paketmanager. Ein Beispiel finden Sie im Amazon Linux 2023 User Guide unter Package Management Tool. Nachdem Sie die schädlichen Pakete entfernt haben, sollten Sie einen Scan durchführen, um sicherzustellen, dass alle Pakete, die möglicherweise durch den bösartigen Code installiert wurden, entfernt wurden. Weitere Informationen finden Sie unter Starten des On-demand Malware-Scans GuardDuty in der.

Die EC2-Instance enthält schädliche Dateien

Bösartige Dateien enthalten schädlichen Code, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Dateien stellen eine aktive und kritische Bedrohung für Ihre Instanz dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Folgen Sie den bewährten Sicherheitsmethoden und entfernen Sie schädliche Dateien, um Ihre Instance vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie schädliche Dateien

Informationen zur Identifizierung des spezifischen Amazon Elastic Block Store (Amazon EBS) - Volumes, das schädliche Dateien enthält, finden Sie im Abschnitt Ressourcen in den Funddetails des Merkmals. Nachdem Sie das Volume mit der schädlichen Datei identifiziert haben, erstellen Sie einen Snapshot des Volumes, bevor Sie Änderungen vornehmen, und entfernen Sie dann die identifizierten schädlichen Dateien. Nachdem Sie die schädlichen Dateien entfernt haben, sollten Sie einen Scan durchführen, um sicherzustellen, dass alle Dateien, die möglicherweise durch die schädliche Datei installiert wurden, entfernt wurden. Weitere Informationen finden Sie unter Starten des On-demand Malware-Scans GuardDuty in der.

Auswirkungsmerkmale für EC2-Instances

Die Wirkungsmerkmale beschreiben den potenziellen Explosionsradius einer Exposition. Security Hub analysiert die effektiven Berechtigungen des mit der EC2-Instance verknüpften AWS Identity and Access Management Principals, um zu ermitteln, auf welche nachgelagerten Ressourcen ein Angreifer zugreifen könnte, wenn die Instance kompromittiert wird, sowie die geschäftliche Bedeutung dieser Ressourcen. Jedes Auswirkungsmerkmal identifiziert ein bestimmtes Muster für die Eskalation von Rechten. Um deinen Explosionsradius zu reduzieren, überprüfe die in den einzelnen Eigenschaften beschriebenen Berechtigungspfade und entferne alle unnötigen Rechte.

Gemäß den üblichen Sicherheitsprinzipien gewähren Sie geringste Rechte, indem Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Ersetzen Sie allgemeine Richtlinien durch spezifische Richtlinien, die nur die spezifischen Aktionen und Ressourcen gewähren, die benötigt werden. Verwenden Sie IAM Access Analyzer, um Empfehlungen auf der Grundlage des Zugriffsverlaufs zu generieren, um ungenutzte zu entfernende Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Ergebnisse für externen und ungenutzten Zugriff und Anwenden von Berechtigungen mit den geringsten Rechten im IAM-Benutzerhandbuch.

Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

Der zugehörige Principal kann einer Rechenressource, die bereits über erweiterte Berechtigungen verfügt, eine Rolle übergeben und Code in diese einschleusen. Auf diese Weise kann der Principal die volle Kontrolle über den Executor erlangen und alle Aktionen ausführen, die die Rolle des Executors zulässt.

Hat einen direkten politischen Eskalationspfad

Der zugehörige Principal kann die IAM-Richtlinien direkt ändern, um sich selbst zusätzliche Berechtigungen zu gewähren und so seine eigenen Rechte ohne Zwischenressourcen zu erweitern.

Hat einen Hijack-Pfad für Vertrauensrichtlinien

Der zugehörige Principal kann die Vertrauensrichtlinie einer IAM-Rolle so ändern, dass er selbst diese Rolle übernehmen kann, wodurch er die Berechtigungen der Rolle erhält.

Hat einen Pfad zur Daten-Ransomware

Der zugehörige Principal kann Daten auf eine Weise verschlüsseln oder löschen, die für Ransomware verwendet werden könnte, z. B. durch Verschlüsseln von Amazon S3 S3-Objekten mit einem vom Kunden verwalteten AWS KMS Schlüssel und anschließendes Ändern der Schlüsselrichtlinie.

Hat den Beschränkungspfad entfernt

Der zugehörige Prinzipal kann Sicherheitseinschränkungen wie Zugriffsgrenzen, Dienststeuerungsrichtlinien oder ressourcenbasierte Policy-Deny-Statements aufheben und so die Möglichkeiten anderer Prinzipale oder der Ressource selbst erweitern.

Hat die Rolle bestanden, den Executor-Pfad erstellen

Der zugehörige Principal kann eine neue Rechenressource (z. B. eine Lambda-Funktion oder eine Amazon EC2 EC2-Instance) erstellen und ihr eine privilegierte Rolle zuweisen, wodurch seine eigenen Berechtigungen durch die neue Ressource effektiv gewaschen werden.

Hat den Executor-Pfad für die Swap-Rolle bereits

Der zugehörige Principal kann die einer vorhandenen Rechenressource zugeordnete IAM-Rolle ändern und sie durch eine privilegiertere Rolle ersetzen, um den Zugriff zu eskalieren.

Hat einen Eskalationspfad für die Rollenkette

Der zugeordnete Principal kann eine Abfolge von Rollen übernehmen, wobei jede Rolle in der Kette über immer umfangreichere Berechtigungen verfügt, sodass letztendlich eine Rolle mit hohen Rechten erreicht wird.

Hat einen privilegierten Executor-Pfad für Inject-Code

Der zugehörige Principal kann Code in eine laufende Rechenressource mit erhöhten Rechten einfügen und dabei beliebige Operationen unter der privilegierten Rolle dieser Ressource ausführen.

Hat den Audit-Trail-Pfad deaktiviert

Der zugehörige Principal kann Protokollierungs- oder Überwachungsdienste deaktivieren CloudTrail, um beispielsweise während oder nach einer Eskalation effektiv seine Spuren zu verwischen.

Hat Zugriff auf den vorhandenen Executor-Pfad

Der zugehörige Principal kann eine bestehende Rechenressource aufrufen oder eine Verbindung zu ihr herstellen und die ihr zugeordnete Rolle verwenden, um privilegierte Aktionen auszuführen.

Hat einen Pfad zum Minting von Anmeldeinformationen

Der zugehörige Prinzipal kann neue langfristige Anmeldeinformationen (wie Zugriffsschlüssel oder Anmeldeprofile) für andere Prinzipale erstellen und so persistente Zugriffspfade einrichten, die Passwortrotationen oder Sitzungsablaufzeiten überstehen.

Hat den Datenzugriffspfad bestanden

Der zugehörige Principal kann eine Dienstressource erstellen und ihr eine Rolle zuweisen, die Zugriff auf vertrauliche Daten hat, sodass er über die neue Ressource indirekt auf diese Daten zugreifen kann.

Hat den Pfad zur Übernahme der Rolle, der Aufgabe

Der zugehörige Principal kann eine Rolle an eine geplante oder ereignisgesteuerte Aufgabe übergeben (z. B. eine Lambda-Funktion, die durch ein Ereignis ausgelöst wird), sodass er beliebigen Code mit den Berechtigungen dieser Rolle ausführen kann.

Hat einen Single-Hop-Datenzugriffspfad

Der zugehörige Principal kann über seine vorhandenen Berechtigungen direkt auf vertrauliche Datenressourcen (wie Amazon S3 S3-Buckets oder DynamoDB-Tabellen) zugreifen, ohne dass zwischengeschaltete Eskalationsschritte erforderlich sind.

Hat einen Pfad zur Weiterentwicklung der Fähigkeiten

Der zugeordnete Principal verfügt über einen Pfad zur Eskalation von Rechten, der seine allgemeinen Fähigkeiten über das hinaus erweitert, was seine direkt zugewiesenen Berechtigungen vermuten lassen würden. Dies ist eine allgemeine Klassifizierung für Pfade, die keinem spezifischeren Muster entsprechen.

Geschäftliche Kritikalität

Die geschäftliche Wichtigkeit der primären Ressource, die entweder durch Automatisierungsregeln oder durch Rückschlüsse aus dem Namen und den Tags festgelegt wird.

Behebung von Risiken für Amazon ECS-Services

AWS Security Hub kann Ergebnisse zur Gefährdung von Amazon Elastic Container Service (Amazon ECS) -Services generieren.

Der Amazon ECS-Service, der an einer Expositionsfeststellung beteiligt war, und seine identifizierenden Informationen sind im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Sie können diese Ressourcendetails auf der Security Hub-Konsole oder programmgesteuert mithilfe der GetFindingsV2Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht

benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einzelnes Problembehebungsergebnis umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

> **Note**
>
> Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- Merkmale von Fehlkonfigurationen für Amazon ECS-Services
  - Der Amazon ECS-Service verwendet eine Aufgabendefinition, die Containern den Zugriff auf die Root-Dateisysteme ermöglicht.
  - Der Amazon ECS-Service verwendet eine Aufgabendefinition, die so konfiguriert ist, dass sie den Prozess-Namespace eines Hosts gemeinsam nutzt.
  - Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit Klartext-Anmeldeinformationen in den Umgebungsvariablen konfiguriert ist.
  - Der Amazon ECS-Service hat eine offene Sicherheitsgruppe
  - Der Amazon ECS-Service hat öffentliche IP-Adressen
  - Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit aktiviertem Host-Netzwerkmodus konfiguriert ist
- Erreichbarkeitsmerkmale für Amazon ECS-Services
  - Der Amazon ECS-Service ist über das Internet erreichbar
- Merkmale der Sicherheitslücke für Amazon ECS-Services
  - Der Amazon ECS-Service verfügt über einen Container mit Softwareschwachstellen, die im Netzwerk ausgenutzt werden können und bei denen die Wahrscheinlichkeit einer Ausnutzung hoch ist

- Der Amazon ECS-Service hat einen Container mit Softwareschwachstellen
- Der Amazon ECS-Service hat einen Container mit einem End-Of-Life Betriebssystem
- Der Amazon ECS-Service hat einen Container mit bösartigen Softwarepaketen

- Wirkungsmerkmale für Amazon ECS-Services
  - Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff
  - Hat einen direkten politischen Eskalationspfad
  - Hat einen Hijack-Pfad für Vertrauensrichtlinien
  - Hat einen Pfad zur Daten-Ransomware
  - Hat den Beschränkungspfad entfernt
  - Hat die Rolle bestanden, den Executor-Pfad erstellen
  - Hat einen bestehenden Executor-Pfad für die Swap-Rolle
  - Hat einen Eskalationspfad für die Rollenkette
  - Hat einen privilegierten Executor-Pfad für Inject-Code
  - Hat den Audit-Trail-Pfad deaktiviert
  - Hat Zugriff auf den vorhandenen Executor-Pfad
  - Hat einen Pfad zum Minting von Anmeldeinformationen
  - Hat den Datenzugriffspfad bestanden
  - Hat den Pfad zur Übernahme der Rolle, der Aufgabe
  - Hat einen Single-Hop-Datenzugriffspfad
  - Hat einen Pfad zur Weiterentwicklung der Fähigkeiten
  - Geschäftliche Kritikalität

Merkmale von Fehlkonfigurationen für Amazon ECS-Services

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Amazon ECS-Services und empfohlene Schritte zur Behebung.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die Containern den Zugriff auf die Root-Dateisysteme ermöglicht.

Amazon ECS-Container mit Zugriff auf das Host-Root-Dateisystem können potenziell kritische Dateien auf dem Hostsystem lesen, ändern oder ausführen. Diese Konfiguration erhöht das Risiko, dass ein kompromittierter Container für den Zugriff auf oder die Änderung von Ressourcen außerhalb

des vorgesehenen Bereichs verwendet werden könnte, wodurch möglicherweise sensible Daten im Host-Dateisystem offengelegt werden. Gemäß den Standardsicherheitsprinzipien gewähren Sie geringste Rechte. Das bedeutet, dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

Problembehebung: Überprüfen und ändern Sie Container mit Zugriff auf das Host-Dateisystem

Identifizieren Sie im Expositionsergebnis den ARN der Aufgabendefinition. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Aufgabendefinition nach dem Abschnitt Volumes, der Host-Pfadzuordnungen definiert.

Überprüfen Sie die Aufgabendefinition, um festzustellen, ob der Zugriff auf das Host-Dateisystem für die Container-Funktionalität erforderlich ist. Wenn kein Zugriff auf das Host-Dateisystem erforderlich ist, erstellen Sie eine neue Version der Aufgabendefinition und entfernen Sie alle Volume-Definitionen, die Hostpfade verwenden. Wenn Zugriff auf das Host-Dateisystem erforderlich ist, sollten Sie erwägen, den Container so zu konfigurieren, dass er ein schreibgeschütztes Dateisystem verwendet, um unbefugte Änderungen zu verhindern.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die so konfiguriert ist, dass sie den Prozess-Namespace eines Hosts gemeinsam nutzt.

Amazon ECS-Container, die mit exponierten Namespaces ausgeführt werden, können potenziell auf Hostsystemressourcen und andere Container-Namespaces zugreifen. Diese Konfiguration könnte es einem kompromittierten Container ermöglichen, seine Isolationsgrenze zu umgehen und auf Prozesse, Netzwerkschnittstellen oder andere Ressourcen außerhalb seines vorgesehenen Bereichs zuzugreifen.

Ein Prozess-ID-Namespace (PID) sorgt für die Trennung zwischen Prozessen. Er verhindert, dass Systemprozesse sichtbar sind, und ermöglicht die Wiederverwendung von PIDs, einschließlich PID 1. Wenn der Host-PID-Namespace von Containern gemeinsam genutzt wird, können Container alle Prozesse auf dem Hostsystem sehen, wodurch die Isolation auf Prozessebene reduziert wird. Dies könnte zu unberechtigtem Zugriff auf Host-Prozesse führen, einschließlich der Möglichkeit, diese zu manipulieren und zu beenden. Halten Sie sich an die üblichen Sicherheitsprinzipien und achten Sie auf eine angemessene Namespace-Isolierung für Container.

Behebung: Aktualisieren Sie Aufgabendefinitionen mit offengelegten Namespaces

Öffnen Sie die Registerkarte Ressourcen der Exposure und identifizieren Sie die Aufgabendefinition mit dem offengelegten Namespace. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie nach den PIDMode-Einstellungen mit dem Wert host, die die Prozess-ID-

Namespaces mit dem Host teilen würden. Entfernen Sie die Einstellungen pidMode: host aus Ihren Aufgabendefinitionen, um sicherzustellen, dass Container mit der richtigen Namespace-Isolierung ausgeführt werden.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit Klartext-Anmeldeinformationen in den Umgebungsvariablen konfiguriert ist.

Amazon ECS-Container mit Klartext-Anmeldeinformationen in Umgebungsvariablen geben vertrauliche Authentifizierungsinformationen preis, die gefährdet werden könnten, wenn ein Angreifer Zugriff auf die Aufgabendefinition, die Containerumgebung oder die Container-Logs erhält. Dies stellt ein erhebliches Sicherheitsrisiko dar, da durchgesickerte Anmeldeinformationen für den Zugriff auf andere AWS Dienste oder Ressourcen verwendet werden könnten.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Ersetzen Sie Klartext-Anmeldeinformationen

Identifizieren Sie bei der Ermittlung der Sicherheitslücke die Aufgabendefinition durch Klartext-Anmeldeinformationen. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Container-Definition nach Umgebungsvariablen, die sensible Werte wie AWS Zugriffsschlüssel, Datenbankkennwörter oder API-Token enthalten.

Erwägen Sie die folgenden Alternativen, um Anmeldeinformationen zu übergeben:

- Anstatt AWS Zugriffsschlüssel zu verwenden, verwenden Sie IAM-Aufgabenausführungsrollen und Aufgabenrollen, um Ihren Containern Berechtigungen zu erteilen.
- Speichern Sie Anmeldeinformationen als Geheimnisse in Ihrer Aufgabendefinition AWS Secrets Manager und verweisen Sie darauf.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition, die Anmeldeinformationen sicher verarbeitet. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Der Amazon ECS-Service hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Amazon ECS-Aufgaben zur Steuerung des eingehenden und ausgehenden Datenverkehrs. Offene Sicherheitsgruppen, die uneingeschränkten

Zugriff von jeder beliebigen IP-Adresse aus ermöglichen, können Ihre Container unberechtigtem Zugriff aussetzen und so das Risiko erhöhen, automatisierten Scan-Tools und gezielten Angriffen ausgesetzt zu werden. Halten Sie sich an die Standardsicherheitsprinzipien und beschränken Sie den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen Sie die Sicherheitsgruppenregeln und bewerten Sie die aktuelle Konfiguration

Öffnen Sie die Ressource für die Amazon ECS-Sicherheitsgruppe. Prüfen Sie, welche Ports offen und von weiten IP-Bereichen aus zugänglich sind, z. `(0.0.0.0/0 or ::/0)` B.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken.

Ändern Sie die Regeln für Sicherheitsgruppen

Ziehen Sie die folgenden Optionen für alternative Zugriffsmethoden in Betracht:

- Session Manager bietet sicheren Shell-Zugriff auf Ihre Amazon EC2 EC2-Instances, ohne dass eingehende Ports erforderlich sind, SSH-Schlüssel verwaltet oder Bastion-Hosts verwaltet werden müssen.
- NACLs bieten eine zusätzliche Sicherheitsebene auf Subnetzebene. Im Gegensatz zu Sicherheitsgruppen sind NACLs zustandslos und erfordern, dass sowohl eingehende als auch ausgehende Regeln explizit definiert werden.

Der Amazon ECS-Service hat öffentliche IP-Adressen

Amazon ECS-Services mit öffentlichen IP-Adressen, die ihren Aufgaben zugewiesen sind, sind direkt über das Internet zugänglich. Dies kann zwar für Dienste erforderlich sein, die öffentlich verfügbar sein müssen, erhöht jedoch die Angriffsfläche und das Potenzial für unbefugten Zugriff.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Identifizieren Sie Dienste mit öffentlichen IP-Adressen

Identifizieren Sie in der Risikofeststellung den Amazon ECS-Service, dem öffentliche IP-Adressen für seine Aufgaben zugewiesen wurden. Suchen Sie in der Servicekonfiguration nach `ENABLED` der `assignPublicIp` Einstellung mit dem Wert von.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition, die öffentliche IP-Adressen deaktiviert. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Implementieren Sie Zugriffsmuster für private Netzwerke

Für Instances, auf denen Webanwendungen ausgeführt werden, sollten Sie die Verwendung eines Load Balancer (LB) in Betracht ziehen. LBs können so konfiguriert werden, dass Ihre Instances in privaten Subnetzen ausgeführt werden können, während der LB in einem öffentlichen Subnetz läuft und den Internetverkehr abwickelt.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit aktiviertem Host-Netzwerkmodus konfiguriert ist

Amazon ECS-Container, die im Host-Netzwerkmodus ausgeführt werden, teilen sich den Netzwerk-Namespace mit dem Host und ermöglichen so den direkten Zugriff auf die Netzwerkschnittstellen, Ports und Routing-Tabellen des Hosts. Diese Konfiguration umgeht die durch Container bereitgestellte Netzwerkisolierung, wodurch Dienste, die auf dem Container ausgeführt werden, möglicherweise direkt externen Netzwerken zugänglich gemacht werden und es Containern ermöglicht, die Netzwerkeinstellungen des Hosts zu ändern. Halten Sie sich an die Standardsicherheitsprinzipien und sorgen Sie für eine angemessene Netzwerkisolierung von Containern.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Deaktivieren Sie den Host-Netzwerkmodus

Identifizieren Sie in der Expositionsanalyse die Aufgabendefinition mit dem Host-Netzwerkmodus. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Aufgabendefinition nach der Einstellung NetworkMode mit dem Wert host.

Ziehen Sie die folgenden Optionen in Betracht, um den Host-Netzwerkmodus zu deaktivieren:

- Der `awsvpc` Netzwerkmodus bietet die stärkste Netzwerkisolierung, indem er jeder Aufgabe eine eigene elastic network interface gibt.
- Der `bridge` Netzwerkmodus bietet Isolierung und ermöglicht gleichzeitig Port-Zuordnungen, um dem Host bestimmte Container-Ports zugänglich zu machen.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition mit der aktualisierten Netzwerkmoduskonfiguration. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Erreichbarkeitsmerkmale für Amazon ECS-Services

Im Folgenden finden Sie Merkmale der Erreichbarkeit für Amazon ECS-Services und empfohlene Schritte zur Problembehebung.

Der Amazon ECS-Service ist über das Internet erreichbar

Ein Amazon ECS-Service, der Aufgaben in einem öffentlichen Subnetz ausführt, ist direkt über das Internet zugänglich. Dies erhöht die Angriffsfläche und das Risiko eines unbefugten Zugriffs. Folgen Sie den Standardsicherheitsprinzipien, führen Sie Aufgaben in privaten Subnetzen aus und gewähren Sie nur den Internetzugang, den Ihr Dienst benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Führen Sie Aufgaben in einem privaten Subnetz aus

Um Ihre Aufgaben aus einem öffentlichen Subnetz zu verlagern, aktualisieren Sie die Netzwerkkonfiguration für Ihren Starttyp:

- Geben Sie für Fargate private Subnetze in der Netzwerkkonfiguration Ihres Amazon ECS-Service an und stellen `assignPublicIp` Sie auf ein. `DISABLED` Amazon ECS hostet jede Aufgabe in einem privaten Subnetz und leitet den ausgehenden Datenverkehr über ein NAT-Gateway weiter, das Sie dem Subnetz zuordnen.
- Starten Sie für EC2 die Container-Instances, die Ihre Clusterkapazität in privaten Subnetzen bereitstellen. Aufgaben nutzen das private Netzwerk des Hosts und leiten ausgehenden Datenverkehr über ein NAT-Gateway weiter.

Verwenden Sie ein NAT-Gateway für den ausgehenden Zugriff

Verwenden Sie für Aufgaben in einem privaten Subnetz, die einen ausgehenden Internetzugang erfordern, ein NAT-Gateway. Sie können ein NAT-Gateway verwenden, damit Aufgaben ausgehende Verbindungen zum Internet aufbauen und eingehende Verbindungen aus dem Internet verhindern können. Weitere Informationen finden Sie unter Amazon ECS-Anwendungen mit dem Internet Connect im Amazon ECS-Entwicklerhandbuch.

Verwenden Sie einen Load Balancer für eingehenden Zugriff

Für Dienste, die Internetverkehr akzeptieren müssen, führen Sie Ihre Aufgaben in privaten Subnetzen hinter einem Load Balancer aus, der in einem öffentlichen Subnetz ausgeführt wird. Um den Schutz vor Web-Exploits und Bots zu erhöhen, ordnen Sie Ihrem Load Balancer die AWS Web Application Firewall (WAF) zu. Weitere Informationen finden Sie unter Verwenden des Lastenausgleichs zur Verteilung des Amazon ECS-Serviceverkehrs im Amazon ECS-Entwicklerhandbuch.

Merkmale der Sicherheitslücke für Amazon ECS-Services

Im Folgenden finden Sie Merkmale der Sicherheitslücke für Amazon ECS und empfohlene Schritte zur Behebung.

Der Amazon ECS-Service verfügt über einen Container mit Softwareschwachstellen, die im Netzwerk ausgenutzt werden können und bei denen die Wahrscheinlichkeit einer Ausnutzung hoch ist

1. Machen Sie sich mit der Gefahr vertraut

   Package von Ergebnissen zu Sicherheitslücken in Paketen werden Softwarepakete in Ihrer AWS Umgebung identifiziert, die Common Vulnerabilities and Exposures (CVEs) ausgesetzt sind. Angreifer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. ECR-Container-Images können Erkenntnisse zu Sicherheitslücken in Paketen enthalten.
2. Korrigieren Sie das Risiko
   a. Paketversion aktualisieren

      Überprüfen Sie die Sicherheitslücke im Paket, die für Ihr ECR-Container-Image gefunden wurde. Aktualisieren Sie die Paketversion wie von Amazon Inspector vorgeschlagen. Weitere Informationen finden Sie unter Anzeigen von Details zu Ihren Amazon Inspector Inspector-Ergebnissen im Amazon Inspector Inspector-Benutzerhandbuch. Im Abschnitt Problembehebung der Suchdetails in der Amazon Inspector Inspector-Konsole erfahren Sie, welche Befehle Sie ausführen können, um das Paket zu aktualisieren.

b. Aktualisieren Sie die Basis-Container-Images

   Erstellen und aktualisieren Sie regelmäßig die Basis-Container-Images, um Ihre Container auf dem neuesten Stand zu halten. Verwenden Sie beim Neuaufbau eines Images keine unnötigen Komponenten, um die Angriffsfläche zu reduzieren. Anweisungen zur Neuerstellung eines Container-Images finden Sie unter Häufig Ihre Images neu erstellen.

Der Amazon ECS-Service hat einen Container mit Softwareschwachstellen

Softwarepakete, die auf Amazon ECS-Containern installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Sicherheitslücken mit niedriger Priorität stellen Sicherheitslücken dar, die im Vergleich zu Sicherheitslücken mit hoher Priorität einen geringeren Schweregrad oder eine geringere Ausnutzbarkeit aufweisen. Obwohl diese Sicherheitslücken ein geringeres unmittelbares Risiko darstellen, können Angreifer diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Aktualisieren Sie die betroffenen Container-Images

Sehen Sie sich den Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des Merkmals an. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten.

Wenden Sie die entsprechenden Abhilfemaßnahmen an, indem Sie die folgenden allgemeinen Richtlinien befolgen:

- Aktualisieren Sie Ihre Container-Images, um gepatchte Versionen der betroffenen Pakete zu verwenden.
- Aktualisieren Sie die betroffenen Abhängigkeiten in Ihrer Anwendung auf die neuesten sicheren Versionen.

Nachdem Sie Ihr Container-Image aktualisiert haben, übertragen Sie es in Ihre Container-Registry und aktualisieren Sie Ihre Amazon ECS-Aufgabendefinition, um das neue Image zu verwenden.

Zukünftige Überlegungen

Um den Sicherheitsstatus Ihrer Container-Images weiter zu verbessern, sollten Sie die Best Practices für Aufgaben und Containersicherheit von Amazon ECS befolgen. Amazon Inspector kann so konfiguriert werden, dass es automatisch nach CVEs in Ihren Containern sucht. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Container so gering wie möglich zu halten.

Der Amazon ECS-Service hat einen Container mit einem End-Of-Life Betriebssystem

Der Amazon ECS-Container basiert auf einem auslaufenden Betriebssystem, das vom ursprünglichen Entwickler nicht mehr unterstützt oder gewartet wird. Dadurch ist der Container Sicherheitslücken und potenziellen Angriffen ausgesetzt. Wenn Betriebssysteme das Ende ihrer Lebensdauer erreichen, stellen die Anbieter in der Regel die Veröffentlichung neuer Sicherheitsempfehlungen ein. Bestehende Sicherheitsempfehlungen können auch aus den Feeds der Anbieter entfernt werden. Infolgedessen könnte Amazon Inspector möglicherweise aufhören, Ergebnisse für bekannte CVEs zu generieren, was zu weiteren Sicherheitslücken führen würde.

Informationen zu Betriebssystemen, deren Lebensdauer abgelaufen ist und die von Amazon Inspector erkannt werden können, finden Sie im Amazon Inspector Inspector-Benutzerhandbuch unter Nicht mehr erhältliche Betriebssysteme.

Behebung: Update auf eine unterstützte Betriebssystemversion

Aktualisieren Sie auf eine unterstützte Version des Betriebssystems. Öffnen Sie im Expositionsnachweis die Ressource, um auf die betroffene Ressource zuzugreifen. Bevor Sie die Betriebssystemversion in Ihrem Container-Image aktualisieren, finden Sie unter Unterstützte Betriebssysteme im Amazon Inspector Inspector-Benutzerhandbuch die verfügbaren Versionen. Dort finden Sie eine Liste der derzeit unterstützten Betriebssystemversionen. Nachdem Sie Ihr Container-Image aktualisiert haben, übertragen Sie es in Ihre Container-Registry und aktualisieren Sie Ihre Amazon ECS-Aufgabendefinition, um das neue Image zu verwenden.

Der Amazon ECS-Service hat einen Container mit bösartigen Softwarepaketen

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihre Amazon ECS-Container-Images dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Folgen Sie den bewährten Sicherheitsmethoden und entfernen Sie bösartige Pakete, um Ihre Container vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie bösartige Pakete

Sehen Sie sich die Informationen zu den bösartigen Paketen im Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des jeweiligen Merkmals an, um mehr über die Bedrohung zu erfahren. Entfernen Sie die identifizierten bösartigen Pakete aus Ihren Container-Images und erstellen Sie sie anschließend neu. Weitere Informationen finden Sie unter ContainerDependency in der AWS Amazon-ECS-API-Referenz.

Nachdem Sie Ihr Container-Image aktualisiert haben, übertragen Sie es in Ihre Container-Registry und aktualisieren Sie Ihre Amazon ECS-Aufgabendefinition, um das neue Image zu verwenden. Weitere Informationen finden Sie unter Aktualisieren einer Amazon ECS-Aufgabendefinition mithilfe der Konsole im AWS Amazon ECS-Entwicklerhandbuch.

Wirkungsmerkmale für Amazon ECS-Services

Die Wirkungsmerkmale beschreiben den potenziellen Explosionsradius einer Exposition. Security Hub analysiert die effektiven Berechtigungen des mit dem Amazon ECS-Service verknüpften AWS Identity and Access Management Principals, um festzustellen, auf welche nachgelagerten Ressourcen ein Angreifer zugreifen könnte, wenn der Service kompromittiert wird, sowie die geschäftliche Bedeutung dieser Ressourcen. Jedes Auswirkungsmerkmal identifiziert ein bestimmtes Muster für die Eskalation von Rechten. Um deinen Explosionsradius zu verringern, überprüfe die in den einzelnen Merkmalen beschriebenen Berechtigungspfade und entferne alle unnötigen Rechte.

Gemäß den üblichen Sicherheitsprinzipien gewähren Sie geringste Rechte, indem Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Ersetzen Sie allgemeine Richtlinien durch spezifische Richtlinien, die nur die spezifischen Aktionen und Ressourcen gewähren, die benötigt werden. Verwenden Sie IAM Access Analyzer, um Empfehlungen auf der Grundlage des Zugriffsverlaufs zu generieren, um ungenutzte zu entfernende Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Ergebnisse für externen und ungenutzten Zugriff und Anwenden von Berechtigungen mit den geringsten Rechten im IAM-Benutzerhandbuch.

Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

Der zugehörige Principal kann einer Rechenressource, die bereits über erweiterte Berechtigungen verfügt, eine Rolle übergeben und Code in diese einschleusen. Auf diese Weise kann der Principal die volle Kontrolle über den Executor erlangen und alle Aktionen ausführen, die die Rolle des Executors zulässt.

Hat einen direkten politischen Eskalationspfad

Der zugehörige Principal kann die IAM-Richtlinien direkt ändern, um sich selbst zusätzliche Berechtigungen zu gewähren und so seine eigenen Rechte ohne Zwischenressourcen zu erweitern.

Hat einen Hijack-Pfad für Vertrauensrichtlinien

Der zugehörige Principal kann die Vertrauensrichtlinie einer IAM-Rolle so ändern, dass er selbst diese Rolle übernehmen kann, wodurch er die Berechtigungen der Rolle erhält.

Hat einen Pfad zur Daten-Ransomware

Der zugehörige Principal kann Daten auf eine Weise verschlüsseln oder löschen, die für Ransomware verwendet werden könnte, z. B. durch Verschlüsseln von Amazon S3 S3-Objekten mit einem vom Kunden verwalteten AWS KMS Schlüssel und anschließendes Ändern der Schlüsselrichtlinie.

Hat den Beschränkungspfad entfernt

Der zugehörige Prinzipal kann Sicherheitseinschränkungen wie Zugriffsgrenzen, Dienststeuerungsrichtlinien oder ressourcenbasierte Policy-Deny-Statements aufheben und so die Möglichkeiten anderer Prinzipale oder der Ressource selbst erweitern.

Hat die Rolle bestanden, den Executor-Pfad erstellen

Der zugehörige Principal kann eine neue Rechenressource (z. B. eine Lambda-Funktion oder eine Amazon EC2 EC2-Instance) erstellen und ihr eine privilegierte Rolle zuweisen, wodurch seine eigenen Berechtigungen durch die neue Ressource effektiv gewaschen werden.

Hat einen bestehenden Executor-Pfad für die Swap-Rolle

Der zugehörige Principal kann die einer vorhandenen Rechenressource zugeordnete IAM-Rolle ändern und sie durch eine privilegiertere Rolle ersetzen, um den Zugriff zu eskalieren.

Hat einen Eskalationspfad für die Rollenkette

Der zugeordnete Principal kann eine Abfolge von Rollen übernehmen, wobei jede Rolle in der Kette über immer umfangreichere Berechtigungen verfügt, sodass letztendlich eine Rolle mit hohen Rechten erreicht wird.

Hat einen privilegierten Executor-Pfad für Inject-Code

Der zugehörige Principal kann Code in eine laufende Rechenressource mit erhöhten Rechten einfügen und dabei beliebige Operationen unter der privilegierten Rolle dieser Ressource ausführen.

Hat den Audit-Trail-Pfad deaktiviert

Der zugehörige Principal kann Protokollierungs- oder Überwachungsdienste deaktivieren CloudTrail, um beispielsweise während oder nach einer Eskalation effektiv seine Spuren zu verwischen.

Hat Zugriff auf den vorhandenen Executor-Pfad

Der zugehörige Principal kann eine bestehende Rechenressource aufrufen oder eine Verbindung zu ihr herstellen und die ihr zugeordnete Rolle verwenden, um privilegierte Aktionen auszuführen.

Hat einen Pfad zum Minting von Anmeldeinformationen

Der zugehörige Prinzipal kann neue langfristige Anmeldeinformationen (wie Zugriffsschlüssel oder Anmeldeprofile) für andere Prinzipale erstellen und so persistente Zugriffspfade einrichten, die Passwortrotationen oder Sitzungsablaufzeiten überstehen.

Hat den Datenzugriffspfad bestanden

Der zugehörige Principal kann eine Dienstressource erstellen und ihr eine Rolle zuweisen, die Zugriff auf vertrauliche Daten hat, sodass er über die neue Ressource indirekt auf diese Daten zugreifen kann.

Hat den Pfad zur Übernahme der Rolle, der Aufgabe

Der zugehörige Principal kann eine Rolle an eine geplante oder ereignisgesteuerte Aufgabe übergeben (z. B. eine Lambda-Funktion, die durch ein Ereignis ausgelöst wird), sodass er beliebigen Code mit den Berechtigungen dieser Rolle ausführen kann.

Hat einen Single-Hop-Datenzugriffspfad

Der zugehörige Principal kann über seine vorhandenen Berechtigungen direkt auf vertrauliche Datenressourcen (wie Amazon S3 S3-Buckets oder DynamoDB-Tabellen) zugreifen, ohne dass zwischengeschaltete Eskalationsschritte erforderlich sind.

Hat einen Pfad zur Weiterentwicklung der Fähigkeiten

Der zugeordnete Principal verfügt über einen Pfad zur Eskalation von Rechten, der seine allgemeinen Fähigkeiten über das hinaus erweitert, was seine direkt zugewiesenen Berechtigungen vermuten

lassen würden. Dies ist eine allgemeine Klassifizierung für Pfade, die keinem spezifischeren Muster entsprechen.

Geschäftliche Kritikalität

Die geschäftliche Wichtigkeit der primären Ressource, die entweder durch Automatisierungsregeln oder durch Rückschlüsse aus dem Namen und den Tags festgelegt wird.

Behebung von Risiken für Amazon EKS-Cluster

AWS Security Hub kann Risikoprüfungen für Amazon Elastic Kubernetes Service (Amazon EKS) - Cluster generieren.

Der Amazon EKS-Cluster, der an einer Gefahrenfeststellung beteiligt war, und seine identifizierenden Informationen sind im Abschnitt „Ressourcen“ der Ermittlungsdetails aufgeführt. Sie können diese Ressourcendetails auf der Security Hub-Konsole oder programmgesteuert mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Gefahrenfeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema enthaltenen Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Ressourcen. AWS

Inhalt

- Merkmale bei der Fehlkonfiguration für Amazon EKS-Cluster
  - Der Amazon EKS-Cluster ermöglicht den öffentlichen Zugriff
  - Der Amazon EKS-Cluster verwendet eine nicht unterstützte Kubernetes-Version

  - Der Amazon EKS-Cluster verwendet unverschlüsselte Kubernetes-Geheimnisse
- Sicherheitsmerkmale für Amazon EKS-Cluster
  - Der Amazon EKS-Cluster verfügt über einen Container mit Software-Sicherheitslücken, die vom Netzwerk ausgenutzt werden können und bei denen eine hohe Wahrscheinlichkeit besteht, dass sie ausgenutzt werden
  - Der Amazon EKS-Cluster verfügt über einen Container mit Software-Sicherheitslücken
  - Der Amazon EKS-Cluster verfügt über einen Container mit einem End-Of-Life Betriebssystem
  - Der Amazon EKS-Cluster verfügt über einen Container mit schädlichen Softwarepaketen
  - Der Amazon EKS-Cluster enthält schädliche Dateien

Merkmale bei der Fehlkonfiguration für Amazon EKS-Cluster

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Amazon EKS-Cluster und empfohlene Korrekturmaßnahmen.

Der Amazon EKS-Cluster ermöglicht den öffentlichen Zugriff

Der Amazon EKS-Cluster-Endpunkt ist der Endpunkt, den Sie für die Kommunikation mit dem Kubernetes-API-Server Ihres Clusters verwenden. Standardmäßig ist dieser Endpunkt im Internet öffentlich zugänglich. Öffentliche Endpunkte erhöhen Ihre Angriffsfläche und erhöhen das Risiko eines unbefugten Zugriffs auf Ihren Kubernetes-API-Server, sodass Angreifer möglicherweise auf Cluster-Ressourcen zugreifen oder diese ändern oder auf vertrauliche Daten zugreifen können. Beschränken Sie den Zugriff auf Ihren Amazon EKS-Cluster-Endpunkt gemäß den bewährten Sicherheitsmethoden auf nur die erforderlichen IP-Bereiche.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Ändern Sie den Endpunktzugriff

Öffnen Sie im Expositionsergebnis die Ressource. Dadurch wird der betroffene Amazon EKS-Cluster geöffnet. Sie können Ihren Cluster so konfigurieren, dass er privaten Zugriff, öffentlichen Zugriff oder beides verwendet.

Bei privatem Zugriff verwenden Kubernetes-API-Anfragen, die aus der VPC Ihres Clusters stammen, den privaten VPC-Endpunkt. Bei öffentlichem Zugriff verwenden Kubernetes-API-Anfragen, die von außerhalb der VPC Ihres Clusters stammen, den öffentlichen Endpunkt.

Ändern oder entfernen Sie den öffentlichen Zugriff auf den Cluster

Informationen zum Ändern des Endpunktzugriffs für einen vorhandenen Cluster finden Sie unter Ändern des Cluster-Endpunktzugriffs im Amazon Elastic Kubernetes Service-Benutzerhandbuch. Implementieren Sie restriktivere Regeln, die auf bestimmten IP-Bereichen oder Sicherheitsgruppen basieren. Wenn ein eingeschränkter öffentlicher Zugriff erforderlich ist, beschränken Sie den Zugriff auf bestimmte CIDR-Blockbereiche oder verwenden Sie Präfixlisten.

Der Amazon EKS-Cluster verwendet eine nicht unterstützte Kubernetes-Version

Amazon EKS unterstützt jede Kubernetes-Version für einen begrenzten Zeitraum. Das Ausführen von Clustern mit nicht unterstützten Kubernetes-Versionen kann Ihre Umgebung Sicherheitslücken aussetzen, da für veraltete Versionen keine CVE-Patches mehr veröffentlicht werden. Nicht unterstützte Versionen können bekannte Sicherheitslücken enthalten, die von Angreifern ausgenutzt werden können, und es fehlen Sicherheitsfunktionen, die in neueren Versionen möglicherweise verfügbar sind. Halten Sie Ihre Kubernetes-Version gemäß den bewährten Sicherheitsmethoden auf dem neuesten Stand.

Abhilfe: Aktualisieren Sie die Kubernetes-Version

Öffnen Sie im Expositionsergebnis die Ressource. Dadurch wird der betroffene Amazon EKS-Cluster geöffnet. Bevor Sie Ihren Cluster aktualisieren, finden Sie im Amazon Elastic Kubernetes Service-Benutzerhandbuch unter Verfügbare Versionen zum Thema Standardunterstützung eine Liste der derzeit unterstützten Kubernetes-Versionen.

Der Amazon EKS-Cluster verwendet unverschlüsselte Kubernetes-Geheimnisse

Kubernetes-Geheimnisse werden standardmäßig unverschlüsselt im dem API-Server zugrunde liegenden Datenspeicher (etcd) gespeichert. Jeder mit API-Zugriff oder Zugriff auf etcd kann ein Geheimnis abrufen oder ändern. Um dies zu verhindern, sollten Sie Kubernetes-Geheimnisse im Ruhezustand verschlüsseln. Wenn Kubernetes-Secrets unverschlüsselt sind, sind sie anfällig für unbefugten Zugriff, falls etcd kompromittiert wird. Da Secrets oft vertrauliche Informationen wie Passwörter und API-Token enthalten, kann ihre Offenlegung zu unbefugtem Zugriff auf andere Anwendungen und Daten führen. Verschlüsseln Sie alle vertraulichen Informationen, die in Kubernetes-Geheimnissen gespeichert sind, und halten Sie sich dabei an die bewährten Sicherheitsmethoden.

Behebung: Verschlüsseln Sie geheime Kubernetes-Geheimnisse

Amazon EKS unterstützt die Verschlüsselung von Kubernetes-Geheimnissen mithilfe von KMS-Schlüsseln durch Umschlagverschlüsselung. Informationen zum Aktivieren der Verschlüsselung von

Kubernetes-Geheimnissen für Ihren EKS-Cluster finden Sie im Amazon EKS-Benutzerhandbuch unter Verschlüsseln von Kubernetes-Geheimnissen mit KMS auf vorhandenen Clustern.

Sicherheitsmerkmale für Amazon EKS-Cluster

Hier sind die Schwachstellenmerkmale für Amazon EKS-Cluster.

Der Amazon EKS-Cluster verfügt über einen Container mit Software-Sicherheitslücken, die vom Netzwerk ausgenutzt werden können und bei denen eine hohe Wahrscheinlichkeit besteht, dass sie ausgenutzt werden

Softwarepakete, die auf Amazon EKS-Clustern installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Kritische CVEs stellen erhebliche Sicherheitsrisiken für Ihre Umgebung dar. AWS Unbefugte Benutzer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Ausnutzungswahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Patchen Sie diese Sicherheitslücken gemäß den bewährten Sicherheitsmethoden, um Ihre Instanz vor Angriffen zu schützen.

Behebung: Aktualisieren Sie die betroffenen Instanzen

Aktualisieren Sie Ihre Container-Images auf neuere Versionen, die Sicherheitsupdates für die identifizierten Sicherheitslücken enthalten. Dies beinhaltet in der Regel die Neuerstellung Ihrer Container-Images mit aktualisierten Basis-Images oder Abhängigkeiten und die anschließende Bereitstellung der neuen Images in Ihrem Amazon EKS-Cluster.

Der Amazon EKS-Cluster verfügt über einen Container mit Software-Sicherheitslücken

Softwarepakete, die auf Amazon EKS-Clustern installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Unkritische CVEs stellen Sicherheitslücken dar, die im Vergleich zu kritischen CVEs einen geringeren Schweregrad oder eine geringere Ausnutzbarkeit aufweisen. Obwohl diese Sicherheitslücken ein geringeres unmittelbares Risiko darstellen, können Angreifer diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Patchen Sie diese Sicherheitslücken gemäß den bewährten Sicherheitsmethoden, um Ihre Instanz vor Angriffen zu schützen.

Behebung: Aktualisieren Sie die betroffenen Instanzen

Aktualisieren Sie Ihre Container-Images auf neuere Versionen, die Sicherheitsupdates für die identifizierten Sicherheitslücken enthalten. Dies beinhaltet in der Regel die Neuerstellung Ihrer Container-Images mit aktualisierten Basis-Images oder Abhängigkeiten und die anschließende Bereitstellung der neuen Images in Ihrem Amazon EKS-Cluster.

Der Amazon EKS-Cluster verfügt über einen Container mit einem End-Of-Life Betriebssystem

Das Amazon EKS-Container-Image basiert auf einem ausgelaufenen Betriebssystem, das vom ursprünglichen Entwickler nicht mehr unterstützt oder gewartet wird. Dadurch ist der Container Sicherheitslücken und potenziellen Angriffen ausgesetzt. Wenn Betriebssysteme das Ende ihrer Lebensdauer erreichen, stellen Anbieter in der Regel die Veröffentlichung neuer Sicherheitshinweise ein. Bestehende Sicherheitshinweise können auch aus den Feeds der Anbieter entfernt werden. Infolgedessen könnte Amazon Inspector möglicherweise die Generierung von Ergebnissen für bekannte CVEs einstellen, was zu weiteren Sicherheitslücken führen würde.

Informationen zu Betriebssystemen, die das Ende ihrer Lebensdauer erreicht haben und die von Amazon Inspector erkannt werden können, finden Sie im Amazon Inspector-Benutzerhandbuch unter Nicht mehr erhältliche Betriebssysteme.

Abhilfe: Aktualisieren Sie auf eine unterstützte Betriebssystemversion

Aktualisieren Sie auf eine unterstützte Version des Betriebssystems. Öffnen Sie im Expositionsergebnis die Ressource, um auf die betroffene Ressource zuzugreifen. Bevor Sie die Betriebssystemversion in Ihrem Container-Image aktualisieren, überprüfen Sie die verfügbaren Versionen unter Unterstützte Betriebssysteme im Amazon Inspector-Benutzerhandbuch. Dort finden Sie eine Liste der aktuell unterstützten Betriebssystemversionen. Nachdem Sie Ihr Container-Image aktualisiert haben, erstellen Sie Ihre Container neu und stellen Sie sie erneut im Amazon EKS-Cluster bereit.

Der Amazon EKS-Cluster verfügt über einen Container mit schädlichen Softwarepaketen

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihren Amazon EKS-Cluster dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Entfernen Sie bösartige Pakete gemäß den bewährten Sicherheitsmethoden, um Ihren Cluster vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie bösartige Pakete

Sehen Sie sich die Details des bösartigen Pakets im Abschnitt „Referenzen“ des Merkmals auf der Registerkarte „Sicherheitslücke“ an, um sich ein Bild von der Bedrohung zu machen. Entfernen Sie die identifizierten schädlichen Pakete aus Ihren Container-Images. Löschen Sie dann die Pods mit dem kompromittierten Image.

Aktualisieren Sie Ihre Kubernetes-Bereitstellungen, um die aktualisierten Container-Images zu verwenden. Stellen Sie dann Ihre Änderungen bereit und stellen Sie Ihre Pods erneut bereit.

Der Amazon EKS-Cluster enthält schädliche Dateien

Bösartige Dateien enthalten schädlichen Code, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Dateien stellen eine aktive und kritische Bedrohung für Ihren Cluster dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Entfernen Sie schädliche Dateien gemäß den bewährten Sicherheitsmethoden, um Ihren Cluster vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie bösartige Dateien

Um das spezifische Amazon Elastic Block Store (Amazon EBS) -Volume zu identifizieren, das schädliche Dateien enthält, überprüfen Sie den Abschnitt Ressourcen in den Funddetails des Merkmals. Nachdem Sie das Volume mit der schädlichen Datei identifiziert haben, entfernen Sie die identifizierten schädlichen Dateien. Nachdem Sie die schädlichen Dateien entfernt haben, sollten Sie erwägen, einen Scan durchzuführen, um sicherzustellen, dass alle Dateien, die möglicherweise durch die schädliche Datei installiert wurden, entfernt wurden. Weitere Informationen finden Sie unter Starten des On-demand Malware-Scans GuardDuty im.

Behebung von Risiken für IAM-Benutzer

AWS Security Hub kann Ergebnisse zur Gefährdung von AWS Identity and Access Management (IAM) -Benutzern generieren.

Auf der Security Hub Hub-Konsole werden der IAM-Benutzer, der an einer Risikofeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen

Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

> **Note**
>
> Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Bewährte IAM-Methoden empfehlen, IAM-Rollen zu erstellen oder einen Verbund mit einem Identitätsanbieter für den Zugriff mit temporären Anmeldeinformationen zu AWS verwenden, anstatt einzelne IAM-Benutzer zu erstellen. Wenn dies für Ihre Organisation und Ihren Anwendungsfall eine Option ist, wechseln Sie zu Rollen oder einem Verbund, anstatt IAM-Benutzer zu verwenden. Weitere Informationen finden Sie unter IAM-Benutzer im IAM-Benutzerhandbuch.

Inhalt

- Merkmale von Fehlkonfigurationen für IAM-Benutzer
  - Der IAM-Benutzer hat MFA nicht aktiviert
  - Das Tool AWS Das Konto für den IAM-Benutzer hat schwache Passwortrichtlinien
  - Der IAM-Benutzer hat ungerichtete Zugriffsschlüssel
  - Der IAM-Benutzer verfügt über eine Richtlinie, die uneingeschränkten Zugriff auf die Entschlüsselung von KMS-Schlüsseln ermöglicht
- Ungenutzte Zugriffsmerkmale für IAM-Benutzer
- Wirkungsmerkmale für IAM-Benutzer
  - Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff
  - Hat einen direkten politischen Eskalationspfad
  - Hat einen Hijack-Pfad für Vertrauensrichtlinien
  - Hat einen Pfad zur Daten-Ransomware
  - Hat den Beschränkungspfad entfernt

- Hat die Rolle bestanden, den Executor-Pfad erstellen
- Hat einen bestehenden Executor-Pfad für die Swap-Rolle
- Hat einen Eskalationspfad für die Rollenkette
- Hat einen privilegierten Executor-Pfad für Inject-Code
- Hat den Audit-Trail-Pfad deaktiviert
- Hat Zugriff auf den vorhandenen Executor-Pfad
- Hat einen Pfad zum Minting von Anmeldeinformationen
- Hat den Datenzugriffspfad bestanden
- Hat den Pfad zur Übernahme der Rolle, der Aufgabe
- Hat einen Single-Hop-Datenzugriffspfad
- Hat einen Pfad zur Weiterentwicklung der Fähigkeiten
- Geschäftliche Kritikalität

Merkmale von Fehlkonfigurationen für IAM-Benutzer

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für IAM-Benutzer und empfohlene Schritte zur Behebung.

Der IAM-Benutzer hat MFA nicht aktiviert

Multi-factor Die Authentifizierung (MFA) bietet zusätzlich zu einem Benutzernamen und einem Passwort eine zusätzliche Schutzebene. Wenn MFA aktiviert ist und sich ein IAM-Benutzer auf einer AWS Website anmeldet, wird er aufgefordert, seinen Benutzernamen, sein Passwort und einen Authentifizierungscode von seinem AWS MFA-Gerät einzugeben. Der authentifizierende Prinzipal muss über ein Gerät verfügen, das einen zeitkritischen Schlüssel ausgibt und Kenntnisse über Anmeldeinformationen haben muss. Ohne MFA erhält ein Angreifer vollen Zugriff auf die Benutzerberechtigungen, wenn das Passwort eines Benutzers AWS kompromittiert wird. Aktivieren Sie MFA gemäß den Standardsicherheitsprinzipien für alle Konten und Benutzer, die AWS-Managementkonsole Zugriff haben.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen Sie die MFA-Typen

AWS unterstützt die folgenden MFA-Typen:

- Passkeys und Sicherheitsschlüssel
- Anwendungen für virtuelle Authentifikatoren
- Hardware-TOTP-Token

Obwohl die Authentifizierung mit einem physischen Gerät in der Regel einen strengeren Sicherheitsschutz bietet, ist die Verwendung einer beliebigen Art von MFA sicherer als die Deaktivierung von MFA.

MFA aktivieren

Informationen zur Aktivierung des MFA-Typs, der Ihren Anforderungen entspricht, finden Sie unter AWS Multi-Faktor-Authentifizierung in IAM im IAM-Benutzerhandbuch. Folgen Sie den Schritten für den spezifischen MFA-Typ, den Sie implementieren möchten. Für Organisationen, die viele Benutzer verwalten, möchten Sie möglicherweise die Verwendung von MFA erzwingen, indem Sie verlangen, dass MFA auf sensible Ressourcen zugreift.

Das Tool AWS Das Konto für den IAM-Benutzer hat schwache Passwortrichtlinien

Passwortrichtlinien tragen zum Schutz vor unbefugtem Zugriff bei, indem sie Mindestanforderungen an die Komplexität von IAM-Benutzerkennwörtern durchsetzen. Ohne strenge Passwortrichtlinien besteht ein erhöhtes Risiko, dass Benutzerkonten durch das Erraten von Passwörtern oder Brute-Force-Angriffe gefährdet werden könnten. Halten Sie sich an die Standardsicherheitsprinzipien und implementieren Sie eine sichere Passwortrichtlinie, um sicherzustellen, dass Benutzer komplexe Passwörter erstellen, die schwer zu erraten sind.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Konfigurieren Sie eine sichere Passwortrichtlinie

Gehen Sie zum IAM-Dashboard und navigieren Sie zu den Kontoeinstellungen. Prüfen Sie die aktuellen Passwortrichtlinien für Ihr Konto, einschließlich der Mindestlänge, der erforderlichen Zeichentypen und der Einstellungen für das Ablaufen von Passwörtern.

Halten Sie sich bei der Festlegung Ihrer Passwortrichtlinie mindestens an die folgenden bewährten Methoden:

- Erfordert mindestens einen Großbuchstaben.
- Erfordert mindestens einen Kleinbuchstaben.

- Erfordert mindestens ein Symbol.
- Erfordert mindestens eine Zahl.
- Erfordert mindestens acht Zeichen.

Zusätzliche Sicherheitsüberlegungen

Ziehen Sie zusätzlich zu einer strengen Passwortrichtlinie die folgenden zusätzlichen Sicherheitsmaßnahmen in Betracht:

- MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem es eine zusätzliche Form der Authentifizierung erfordert. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden.
- Einrichtung von Bedingungselementen, um einzuschränken, wann und wie Administratorberechtigungen verwendet werden können, basierend auf Faktoren wie Quell-IP oder MFA-Alter.

Der IAM-Benutzer hat ungerichtete Zugriffsschlüssel

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel, die den programmatischen Zugriff auf Ressourcen ermöglichen. AWS Wenn Zugriffsschlüssel über einen längeren Zeitraum unverändert bleiben, erhöhen sie das Risiko eines unbefugten Zugriffs, wenn sie kompromittiert werden. Halten Sie sich an bewährte Sicherheitsmethoden und wechseln Sie die Zugangsschlüssel alle 90 Tage, um das Zeitfenster zu minimieren, in dem Angreifer kompromittierte Anmeldeinformationen verwenden können.

Abhilfe: Zugangsschlüssel rotieren

Öffnen Sie im Expositionsnachweis die Ressource. Dadurch wird das Fenster mit den Benutzerdetails geöffnet. Informationen zur Rotation von Zugriffsschlüsseln finden Sie unter Zugriffsschlüssel für IAM-Benutzer verwalten im IAM-Benutzerhandbuch.

Der IAM-Benutzer verfügt über eine Richtlinie, die uneingeschränkten Zugriff auf die Entschlüsselung von KMS-Schlüsseln ermöglicht

AWS KMS ermöglicht es Ihnen, kryptografische Schlüssel zu erstellen und zu verwalten, die zum Schutz Ihrer Daten verwendet werden. IAM-Richtlinien, die uneingeschränkte AWS KMS Entschlüsselungsberechtigungen (z. B. `kms:Decrypt` oder`kms:ReEncryptFrom`) für alle KMS-Schlüssel zulassen, können zu unberechtigtem Datenzugriff führen, wenn die

Anmeldeinformationen eines IAM-Benutzers kompromittiert werden. Wenn sich ein Angreifer Zugriff auf diese Anmeldeinformationen verschafft, könnte er möglicherweise alle verschlüsselten Daten in Ihrer Umgebung entschlüsseln, zu denen auch vertrauliche Daten gehören könnten. Halten Sie sich an bewährte Sicherheitsmethoden und implementieren Sie die geringsten Rechte, indem Sie die AWS KMS Entschlüsselungsberechtigungen auf bestimmte Schlüssel beschränken, die Benutzer für ihre Aufgaben benötigen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Implementieren der geringstmöglichen Zugriffsrechte

Öffnen Sie in der Ermittlung des Risikos die Ressource. Dadurch wird das Fenster „IAM-Richtlinie“ geöffnet. Suchen Sie in KMS nach Berechtigungen, die kms:Decrypt oder `kms:ReEncryptFrom` oder `KMS:*` mit der Ressourcenspezifikation von zulassen. `"*"`

Aktualisieren Sie die Richtlinie, um die AWS KMS Entschlüsselungsberechtigungen auf die jeweils benötigten Schlüssel zu beschränken. Ändern Sie die Richtlinie, um die `"*"` Ressource durch die spezifischen ARNs der erforderlichen AWS KMS Schlüssel zu ersetzen.

Überlegungen zur sicheren Konfiguration

Erwägen Sie, Bedingungen hinzuzufügen, um weiter einzuschränken, wann diese Berechtigungen verwendet werden können. Sie können beispielsweise Entschlüsselungsvorgänge auf bestimmte VPC-Endpunkte oder Quell-IP-Bereiche beschränken. Sie können auch Schlüsselrichtlinien konfigurieren, um weiter einzuschränken, wer bestimmte KMS-Schlüssel verwenden kann.

Ungenutzte Zugriffsmerkmale für IAM-Benutzer

Wenn ein IAM-Benutzer über ungenutzte Berechtigungen, Zugriffsschlüssel oder Passwörter verfügt, kann Security Hub diese als kontextuelle Merkmale in die Risikopergebnisse für diesen Benutzer einbeziehen. Diese Merkmale werden vom vom Service verwalteten IAM Access Analyzer generiert und bieten zusätzlichen Kontext über die Sicherheitslage des Benutzers. Ungenutzte Zugriffsmerkmale sind nicht die Hauptursache für die Entdeckung der Sicherheitslücke, sie weisen jedoch darauf hin, dass der Benutzer über mehr Berechtigungen verfügt als erforderlich, was die potenziellen Auswirkungen erhöht, wenn die Anmeldeinformationen des Benutzers kompromittiert werden.

Insbesondere für ungenutzte Berechtigungen können Sie eine Richtlinienempfehlung mit den geringsten Rechten erstellen, die Ihnen eine detaillierte Ersatzrichtlinie aufzeigt. Weitere Informationen finden Sie unter the section called “Politische Empfehlungen”.

Wirkungsmerkmale für IAM-Benutzer

Die Wirkungsmerkmale beschreiben den potenziellen Explosionsradius einer Exposition. Security Hub analysiert die effektiven Berechtigungen des mit dem IAM-Benutzer verknüpften AWS Identity and Access Management Prinzipals, um festzustellen, auf welche nachgelagerten Ressourcen ein Angreifer zugreifen könnte, wenn der IAM-Benutzer kompromittiert wird, sowie die geschäftliche Bedeutung dieser Ressourcen. Jedes Auswirkungsmerkmal identifiziert ein bestimmtes Muster für die Eskalation von Rechten. Um deinen Explosionsradius zu verringern, überprüfe die in den einzelnen Merkmalen beschriebenen Berechtigungspfade und entferne alle unnötigen Rechte.

Gemäß den üblichen Sicherheitsprinzipien gewähren Sie geringste Rechte, indem Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Ersetzen Sie allgemeine Richtlinien durch spezifische Richtlinien, die nur die spezifischen Aktionen und Ressourcen gewähren, die benötigt werden. Verwenden Sie IAM Access Analyzer, um Empfehlungen auf der Grundlage des Zugriffsverlaufs zu generieren, um ungenutzte zu entfernende Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Ergebnisse für externen und ungenutzten Zugriff und Anwenden von Berechtigungen mit den geringsten Rechten im IAM-Benutzerhandbuch.

Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

Der zugehörige Principal kann einer Rechenressource, die bereits über erweiterte Berechtigungen verfügt, eine Rolle übergeben und Code in diese einschleusen. Auf diese Weise kann der Principal die volle Kontrolle über den Executor erlangen und alle Aktionen ausführen, die die Rolle des Executors zulässt.

Hat einen direkten politischen Eskalationspfad

Der zugehörige Principal kann die IAM-Richtlinien direkt ändern, um sich selbst zusätzliche Berechtigungen zu gewähren und so seine eigenen Rechte ohne Zwischenressourcen zu erweitern.

Hat einen Hijack-Pfad für Vertrauensrichtlinien

Der zugehörige Principal kann die Vertrauensrichtlinie einer IAM-Rolle so ändern, dass er selbst diese Rolle übernehmen kann, wodurch er die Berechtigungen der Rolle erhält.

Hat einen Pfad zur Daten-Ransomware

Der zugehörige Principal kann Daten auf eine Weise verschlüsseln oder löschen, die für Ransomware verwendet werden könnte, z. B. durch Verschlüsseln von Amazon S3 S3-Objekten mit einem vom Kunden verwalteten AWS KMS Schlüssel und anschließendes Ändern der Schlüsselrichtlinie.

Hat den Beschränkungspfad entfernt

Der zugehörige Prinzipal kann Sicherheitseinschränkungen wie Zugriffsgrenzen, Dienststeuerungsrichtlinien oder ressourcenbasierte Policy-Deny-Statements aufheben und so die Möglichkeiten anderer Prinzipale oder der Ressource selbst erweitern.

Hat die Rolle bestanden, den Executor-Pfad erstellen

Der zugehörige Principal kann eine neue Rechenressource (z. B. eine Lambda-Funktion oder eine Amazon EC2 EC2-Instance) erstellen und ihr eine privilegierte Rolle zuweisen, wodurch seine eigenen Berechtigungen durch die neue Ressource effektiv gewaschen werden.

Hat einen bestehenden Executor-Pfad für die Swap-Rolle

Der zugehörige Principal kann die einer vorhandenen Rechenressource zugeordnete IAM-Rolle ändern und sie durch eine privilegiertere Rolle ersetzen, um den Zugriff zu eskalieren.

Hat einen Eskalationspfad für die Rollenkette

Der zugeordnete Principal kann eine Abfolge von Rollen übernehmen, wobei jede Rolle in der Kette über immer umfangreichere Berechtigungen verfügt, sodass letztendlich eine Rolle mit hohen Rechten erreicht wird.

Hat einen privilegierten Executor-Pfad für Inject-Code

Der zugehörige Principal kann Code in eine laufende Rechenressource mit erhöhten Rechten einfügen und dabei beliebige Operationen unter der privilegierten Rolle dieser Ressource ausführen.

Hat den Audit-Trail-Pfad deaktiviert

Der zugehörige Principal kann Protokollierungs- oder Überwachungsdienste deaktivieren CloudTrail, um beispielsweise während oder nach einer Eskalation effektiv seine Spuren zu verwischen.

Hat Zugriff auf den vorhandenen Executor-Pfad

Der zugehörige Principal kann eine bestehende Rechenressource aufrufen oder eine Verbindung zu ihr herstellen und die ihr zugeordnete Rolle verwenden, um privilegierte Aktionen auszuführen.

Hat einen Pfad zum Minting von Anmeldeinformationen

Der zugehörige Principal kann neue langfristige Anmeldeinformationen (wie Zugriffsschlüssel oder Anmeldeprofile) für andere Prinzipale erstellen und so persistente Zugriffspfade einrichten, die Passwortrotationen oder Sitzungsabläufe überstehen.

Hat den Datenzugriffspfad bestanden

Der zugehörige Principal kann eine Dienstressource erstellen und ihr eine Rolle zuweisen, die Zugriff auf vertrauliche Daten hat, sodass er über die neue Ressource indirekt auf diese Daten zugreifen kann.

Hat den Pfad zur Übernahme der Rolle, der Aufgabe

Der zugehörige Principal kann eine Rolle an eine geplante oder ereignisgesteuerte Aufgabe übergeben (z. B. eine Lambda-Funktion, die durch ein Ereignis ausgelöst wird), sodass er beliebigen Code mit den Berechtigungen dieser Rolle ausführen kann.

Hat einen Single-Hop-Datenzugriffspfad

Der zugehörige Principal kann über seine vorhandenen Berechtigungen direkt auf vertrauliche Datenressourcen (wie Amazon S3 S3-Buckets oder DynamoDB-Tabellen) zugreifen, ohne dass zwischengeschaltete Eskalationsschritte erforderlich sind.

Hat einen Pfad zur Weiterentwicklung der Fähigkeiten

Der zugeordnete Principal verfügt über einen Pfad zur Eskalation von Rechten, der seine allgemeinen Fähigkeiten über das hinaus erweitert, was seine direkt zugewiesenen Berechtigungen vermuten lassen würden. Dies ist eine allgemeine Klassifizierung für Pfade, die keinem spezifischeren Muster entsprechen.

Geschäftliche Kritikalität

Die geschäftliche Wichtigkeit der primären Ressource, die entweder durch Automatisierungsregeln oder durch Rückschlüsse aus dem Namen und den Tags festgelegt wird.

Behebung von Risiken für AWS Lambda Funktionen

AWS Security Hub kann Expositionsergebnisse für AWS Lambda Funktionen generieren.

In der Security Hub Hub-Konsole sind die Lambda-Funktion, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einzelnes Problembehebungsergebnis umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

> **Note**
>
> Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- Fehlkonfigurationsmerkmale für Lambda-Funktionen
  - Die Lambda-Funktion wird außerhalb einer Amazon VPC bereitgestellt
  - Die Lambda-Funktion ist über API Gateway ohne Autorisierung zugänglich
  - Die Lambda-Funktion wird über ein Amazon AgentCore Bedrock-Gateway verfügbar gemacht, ohne dass ein Autorisierer konfiguriert ist
  - Die Lambda-Funktion wird über ein Amazon AgentCore Bedrock-Gateway bereitgestellt, das einen nicht authentifizierten öffentlichen Zugriff ermöglicht
- Erreichbarkeitsmerkmale für Lambda-Funktionen

- Die Lambda-Funktion kann öffentlich aufgerufen werden
- Schwachstellenmerkmale für Lambda-Funktionen
  - Die Lambda-Funktion weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können
  - Die Lambda-Funktion weist Softwareschwachstellen auf
  - Die Lambda-Funktion enthält schädliche Softwarepakete
  - Die Lambda-Funktion weist Code-Schwachstellen auf
- Auswirkungsmerkmale für Lambda-Funktionen
  - Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff
  - Hat einen direkten politischen Eskalationspfad
  - Hat einen Hijack-Pfad für Vertrauensrichtlinien
  - Hat einen Pfad zur Daten-Ransomware
  - Hat den Beschränkungspfad entfernt
  - Hat die Rolle bestanden, den Executor-Pfad erstellen
  - Hat einen bestehenden Executor-Pfad für die Swap-Rolle
  - Hat einen Eskalationspfad für die Rollenkette
  - Hat einen privilegierten Executor-Pfad für Inject-Code
  - Hat den Audit-Trail-Pfad deaktiviert
  - Hat Zugriff auf den vorhandenen Executor-Pfad
  - Hat einen Pfad zum Minting von Anmeldeinformationen
  - Hat den Datenzugriffspfad bestanden
  - Hat den Pfad zur Übernahme der Rolle, der Aufgabe
  - Hat einen Single-Hop-Datenzugriffspfad
  - Hat einen Pfad zur Weiterentwicklung der Fähigkeiten
  - Geschäftliche Kritikalität

Fehlkonfigurationsmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Lambda-Funktionen und empfohlene Schritte zur Behebung.

Die Lambda-Funktion wird außerhalb einer Amazon VPC bereitgestellt

Lambda-Funktionen werden standardmäßig mit Zugriff auf das öffentliche Internet bereitgestellt. Diese Standardkonfiguration gibt Lambda-Funktionen die Möglichkeit, AWS Service-Endpunkte und externe APIs zu erreichen, setzt sie aber auch potenziellen Sicherheitsrisiken aus. Funktionen mit Internetzugang könnten verwendet werden, um Daten zu exfiltrieren, mit nicht autorisierten Servern zu kommunizieren oder, falls sie kompromittiert werden, zu Einfallspunkten für externe Akteure zu werden. Amazon VPC bietet Netzwerkisolierung, indem es Ihre Lambda-Funktionen so einschränkt, dass sie nur mit Ressourcen innerhalb Ihres definierten privaten Netzwerks kommunizieren. Stellen Sie Lambda-Funktionen gemäß den Standardsicherheitsprinzipien innerhalb einer VPC bereit, um die Sicherheit durch Netzwerkisolierung zu verbessern.

Behebung: Funktion an VPC anhängen

Wählen Sie in der Risikoprüfung den Link zur Ressource aus. Dadurch wird die Lambda-Funktion in der Lambda-Konsole geöffnet. Um Ihre Lambda-Funktion zu sichern, indem Sie ihren Netzwerkzugriff einschränken, verbinden Sie sie mit einer VPC, die über die entsprechenden Netzwerksteuerungen verfügt.

Bevor Sie Ihre Funktion an eine VPC anhängen, sollten Sie den eventuell benötigten AWS Servicezugriff einplanen, da Funktionen in privaten Subnetzen ohne NAT-Gateways oder VPC-Endpunkte die Service-APIs nicht erreichen können. AWS Informationen zum Anhängen einer Lambda-Funktion an eine Amazon VPC in Ihrem Konto finden Sie unter Lambda-Funktionen an eine Amazon VPC anhängen in Ihrem. AWS-Konto Erwägen Sie die Verwendung von VPC-Endpunkten für die Dienstkonnektivität ohne Internetzugang, wenn Ihre Funktion den Zugriff auf AWS Dienste innerhalb eines privaten Subnetzes erfordert. Konfigurieren Sie ein NAT-Gateway, wenn Sie ausgehende Internetkonnektivität von privaten Subnetzen benötigen.

Die Lambda-Funktion ist über API Gateway ohne Autorisierung zugänglich

API Gateway-Methoden ohne Autorisierung ermöglichen es jedem Anrufer mit Zugriff auf das API Gateway, die integrierte Lambda-Funktion ohne Identitätsprüfung aufzurufen. Diese Konfiguration birgt Sicherheitsrisiken, da Aufrufer die Lambda-Funktion ohne entsprechende Autorisierung aufrufen können, was möglicherweise zum Missbrauch von Funktionsfunktionen, zum Ressourcenverbrauch, zum Zugriff auf sensible Daten oder zu nicht autorisierten Vorgängen führen kann. API Gateway kann zwar über Zugriffskontrollen auf Netzwerkebene verfügen, das Fehlen einer Autorisierung auf Methodenebene könnte jedoch den freien Aufruf der Funktion durch jeden Anrufer mit Netzwerkzugriff auf das API Gateway ermöglichen. Implementieren Sie gemäß den bewährten

Sicherheitsmethoden geeignete Autorisierungsmechanismen für API-Gateway-Methoden, die in Lambda-Funktionen integriert sind.

Behebung: Konfiguration der API-Gateway-Authentifizierung

Wählen Sie auf der Registerkarte Ressourcen der Exposure den Ressourcenlink aus, um auf die API Gateway Gateway-Methode zuzugreifen. Überprüfen Sie die aktuelle Autorisierungskonfiguration und implementieren Sie die entsprechenden Authentifizierungsmechanismen.

API Gateway unterstützt mehrere Authentifizierungsoptionen, darunter AWS IAM, Amazon Cognito Cognito-Benutzerpools, Lambda-Autorisierer und API-Schlüssel. Wählen Sie die Authentifizierungsmethode, die Ihren Sicherheitsanforderungen und Ihrem Anwendungsfall am besten entspricht. Ausführliche Anweisungen zur Konfiguration der Authentifizierung finden Sie unter Steuern und Verwalten des Zugriffs auf eine REST-API in API Gateway im API Gateway Developer Guide.

Die Lambda-Funktion wird über ein Amazon AgentCore Bedrock-Gateway verfügbar gemacht, ohne dass ein Autorisierer konfiguriert ist

Amazon Bedrock AgentCore Gateways stellen Lambda-Funktionen als Tools bereit, die KI-Agenten erkennen und aufrufen können. Ein Gateway ohne Autorisierer akzeptiert Anfragen, ohne die Identität des Anrufers zu überprüfen. Jeder Anrufer, der den Gateway-Endpunkt erhält, kann die Tools auflisten, die das Gateway bereitstellt, und die integrierte Lambda-Funktion ohne Authentifizierung aufrufen. Dies birgt Sicherheitsrisiken, da nicht authentifizierte Aufrufe zum Missbrauch von Funktionsfunktionen, zum Zugriff auf vertrauliche Daten oder zu unbefugten Vorgängen in Ihrer Umgebung führen können. Folgen Sie den bewährten Sicherheitsmethoden und konfigurieren Sie die eingehende Autorisierung auf Amazon AgentCore Bedrock-Gateways, die Lambda-Funktionen unterstützen.

Problembehebung: Konfigurieren Sie die Gateway-Autorisierung für eingehenden Datenverkehr

Notieren Sie sich im Abschnitt Ressourcen der Sicherheitslücke die Gateway-ID. Öffnen Sie die Amazon AgentCore Bedrock-Konsole, wählen Sie das Gateway aus und überprüfen Sie die Konfiguration der eingehenden Autorisierung.

Amazon Bedrock AgentCore Gateways unterstützen eingehende Autorisierung mit einem JSON Web Token (JWT) -Autorisierer über einen OAuth-compliant Identitätsanbieter wie Amazon Cognito. Konfigurieren Sie einen Authorizer so, dass das Gateway das Token des Anrufers validiert, bevor es Tool-Anfragen bearbeitet. Eine ausführliche Anleitung finden Sie unter Voraussetzungen für

die Nutzung des Amazon Bedrock AgentCore Gateway-Service im Amazon Bedrock AgentCore Developer Guide.

Die Lambda-Funktion wird über ein Amazon AgentCore Bedrock-Gateway bereitgestellt, das einen nicht authentifizierten öffentlichen Zugriff ermöglicht

Amazon Bedrock AgentCore Gateways können über eine ressourcenbasierte Richtlinie verfügen, die steuert, welche Principals das Gateway aufrufen können. Eine Gateway-Richtlinie, die „*“ als Principal enthält, ermöglicht es jedem Aufrufer, die Tools aufzurufen, die das Gateway zur Verfügung stellt, einschließlich der integrierten Lambda-Funktion. Diese Konfiguration umgeht identitätsbasierte Zugriffskontrollen und birgt ein erhebliches Risiko, da nicht authentifizierte Anrufer die Funktion aufrufen können. Dies könnte zum Missbrauch von Funktionsfunktionen, zum Zugriff auf vertrauliche Daten oder zu unbefugten Vorgängen führen. Halten Sie sich an bewährte Sicherheitsmethoden und beschränken Sie den Gateway-Zugriff nur auf autorisierte Principals.

Problembehebung: Schränken Sie die ressourcenbasierte Gateway-Richtlinie ein

Öffnen Sie das Gateway, das im Abschnitt Ressourcen der Risikofeststellung angegeben ist, und überprüfen Sie die entsprechende ressourcenbasierte Richtlinie. Entfernen Sie Aussagen, die „*“ als Hauptwort zulassen. Gewähren Sie nur den spezifischen AWS Konto-IDs oder IAM-Prinzipalen Zugriff, die das Gateway aufrufen müssen.

Weitere Informationen zur Beschränkung des Zugriffs auf Amazon Bedrock AgentCore Gateways finden Sie unter Fine-grained Zugriffskontrolle für Amazon Bedrock AgentCore Gateway im Amazon Bedrock Developer Guide. AgentCore

Erreichbarkeitsmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Merkmale zur Erreichbarkeit von Lambda-Funktionen und empfohlene Schritte zur Problembehebung.

Die Lambda-Funktion kann öffentlich aufgerufen werden

Ressourcenbasierte Lambda-Richtlinien bestimmen, wer Ihre Funktionen aufrufen kann. Eine Funktion mit einer Ressourcenrichtlinie, die „*“ als Prinzipal (oder gar keinen Prinzipal) enthält, ermöglicht es allen authentifizierten AWS Benutzern, sie aufzurufen. Dies stellt ein erhebliches Risiko dar, insbesondere bei Funktionen, die vertrauliche Daten verarbeiten, Ressourcen ändern oder über erweiterte Berechtigungen verfügen. Unbefugte Benutzer könnten diese Konfiguration ausnutzen, um unerwünschte Operationen auszuführen, wodurch möglicherweise Daten offengelegt,

Ressourcen manipuliert oder Funktionsfunktionen missbraucht werden. Halten Sie sich an bewährte Sicherheitsmethoden und beschränken Sie den Zugriff auf Lambda-Funktionen nur auf autorisierte Prinzipale.

Behebung: Ändern Sie die ressourcenbasierte Richtlinie der Funktion

Öffnen Sie auf der Registerkarte Ressourcen der Exposition die Ressource mit dem Hyperlink. Dadurch wird die Lambda-Funktion in der Lambda-Konsole geöffnet. Beschränken Sie den Zugriff auf Ihre Lambda-Funktion, indem Sie in der ressourcenbasierten Richtlinie nur autorisierte AWS Konto-IDs oder bestimmte IAM-Prinzipale (Benutzer, Rollen oder Dienste) angeben. Sie können ressourcenbasierte Richtlinien nur programmgesteuert ändern.

Schwachstellenmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Schwachstellenmerkmale für Lambda-Funktionen und empfohlene Schritte zur Behebung.

Die Lambda-Funktion weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können

Softwarepakete, die im Lambda-Funktionscode verwendet werden, können Common Vulnerabilities and Exposures (CVEs) enthalten, bei denen die Wahrscheinlichkeit hoch ist, dass sie ausgenutzt werden. Kritische CVEs stellen erhebliche Sicherheitsrisiken für Ihre Umgebung dar. AWS Angreifer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Wahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Folgen Sie den bewährten Sicherheitsvorkehrungen und patchen Sie diese Sicherheitslücken, um Ihre Funktion vor Angriffen zu schützen.

Behebung: Aktualisieren Sie die betroffenen Funktionen

Suchen Sie im Abschnitt „Referenzen“ auf der Registerkarte „Sicherheitslücke“ nach dem Merkmal. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Aktualisieren Sie die anfälligen Bibliotheken gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen.

In der Regel hängt der Korrektur-Workflow davon ab, ob Sie das Lambda-Paket bereitgestellt haben, indem Sie eine ZIP-Datei hochgeladen oder eine Lambda-Funktion mit einem Container-Image erstellt haben. Nachdem Sie die Bibliotheken aktualisiert haben, aktualisieren Sie den Lambda-

Funktionscode, um die feste Version zu verwenden. Stellen Sie anschließend die aktualisierte Version bereit.

Die Lambda-Funktion weist Softwareschwachstellen auf

Lambda-Funktionen verwenden häufig Bibliotheken und Abhängigkeiten von Drittanbietern, die im Vergleich zu kritischen CVEs Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit enthalten können. Auch wenn diese unkritischen Sicherheitslücken möglicherweise nicht sofort ausgenutzt werden können, stellen sie dennoch Sicherheitslücken dar, die mit anderen Sicherheitslücken verkettet werden können, um Ihre Funktion zu gefährden. Im Laufe der Zeit könnten auch neue Exploit-Techniken auftauchen, die das Risiko dieser Sicherheitslücken erhöhen. Patchen Sie diese Sicherheitslücken gemäß den üblichen Sicherheitsprinzipien, um eine sichere Umgebung aufrechtzuerhalten.

Behebung: Aktualisieren Sie die betroffenen Funktionen

Suchen Sie im Abschnitt „Referenzen“ auf der Registerkarte „Sicherheitslücke“ nach dem Merkmal. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Aktualisieren Sie die anfälligen Bibliotheken gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen.

In der Regel hängt der Korrektur-Workflow davon ab, ob Sie das Lambda-Paket bereitgestellt haben, indem Sie eine ZIP-Datei hochgeladen oder eine Lambda-Funktion mit einem Container-Image erstellt haben. Nachdem Sie die Bibliotheken aktualisiert haben, aktualisieren Sie den Lambda-Funktionscode, um die feste Version zu verwenden. Stellen Sie anschließend die aktualisierte Version bereit.

Die Lambda-Funktion enthält schädliche Softwarepakete

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihre Lambda-Funktion dar, da Angreifer bösartigen Code automatisch ausführen können, ohne eine Sicherheitslücke auszunutzen. Entfernen Sie schädliche Pakete gemäß den bewährten Sicherheitsmethoden, um Ihre Lambda-Funktion vor potenziellen Angriffen zu schützen.

Problembehebung: Entfernen Sie bösartige Pakete

Sehen Sie sich die Informationen zu den bösartigen Paketen im Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des jeweiligen Merkmals an, um mehr über die Bedrohung zu

erfahren. Entfernen Sie die identifizierten bösartigen Pakete aus Ihrem Funktionscode und Ihren Abhängigkeiten. Überprüfen Sie bei Funktionen, die Ebenen verwenden, ob die schädlichen Pakete in irgendwelchen Ebenen installiert sind, und entfernen Sie sie.

Aktualisieren Sie Ihr Bereitstellungspaket oder Container-Image, um die bösartigen Pakete auszuschließen, und stellen Sie dann die aktualisierte Version bereit. Anweisungen finden Sie unter Bereitstellen von Lambda-Funktionen als ZIP-Dateiarchive für .zip-Dateiarchive oder Erstellen einer Lambda-Funktion mithilfe eines Container-Images für Container-Images.

Die Lambda-Funktion weist Code-Schwachstellen auf

Der Anwendungscode der Lambda-Funktion enthält Sicherheitslücken, die von Bedrohungsakteuren ausgenutzt werden könnten. Zu den Sicherheitslücken im Code gehören Datenlecks, Injektionsfehler, fehlende Verschlüsselung und schwache Kryptografie, die durch automatisierte Codeanalyse identifiziert werden. Diese Sicherheitslücken stellen Sicherheitsrisiken für Ihre AWS Umgebung dar, da Angreifer sie ausnutzen können, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Code-Schwachstellen stellen Sicherheitslücken dar, die mit anderen Angriffsvektoren verkettet werden können, um Ihre Funktion zu gefährden. Folgen Sie den bewährten Sicherheitsmethoden und beheben Sie diese Code-Schwachstellen, um Ihre Funktion vor Angriffen zu schützen.

Behebung: Aktualisieren Sie die betroffenen Funktionen

Sehen Sie sich den Abschnitt „Referenzen“ auf der Registerkarte „Sicherheitslücke“ des Merkmals an. Die Ergebnisse von Amazon Inspector können spezifische Anleitungen zur Problembehebung und Codefragmente enthalten, die die anfälligen Codestellen aufzeigen. Beheben Sie die identifizierten Sicherheitsprobleme in Ihrem Funktionscode mithilfe der mitgelieferten Plug-and-Play-Codeblöcke oder durch die Implementierung sicherer Codierungsmethoden.

Lesen Sie immer die Vorschläge zur Codekorrektur, bevor Sie sie übernehmen, da Sie sie möglicherweise bearbeiten müssen, um sicherzustellen, dass Ihr Code wie beabsichtigt funktioniert. Nachdem Sie die Sicherheitslücken behoben haben, aktualisieren Sie den Lambda-Funktionscode, um die korrigierte Version zu verwenden. Anweisungen finden Sie unter Aktualisieren des Funktionscodes im AWS Lambda Entwicklerhandbuch.

Stellen Sie anschließend die aktualisierte Version bereit. Anweisungen finden Sie unter Bereitstellen von Lambda-Funktionen als ZIP-Dateiarchive für .zip-Dateiarchive oder Erstellen einer Lambda-Funktion mithilfe eines Container-Images für Container-Images. Weitere Informationen zum Scannen von Amazon Inspector-Code finden Sie unter Amazon Inspector Lambda-Code-Scanning im Amazon Inspector Inspector-Benutzerhandbuch.

Auswirkungsmerkmale für Lambda-Funktionen

Wirkungsmerkmale beschreiben den potenziellen Explosionsradius einer Exposition. Security Hub analysiert die effektiven Berechtigungen des AWS Identity and Access Management Prinzipals, der mit der Lambda-Funktion verknüpft ist, um zu ermitteln, auf welche nachgelagerten Ressourcen ein Angreifer zugreifen könnte, wenn die Funktion gefährdet ist, sowie die geschäftliche Bedeutung dieser Ressourcen. Jedes Auswirkungsmerkmal identifiziert ein bestimmtes Muster für die Eskalation von Rechten. Um deinen Explosionsradius zu verringern, überprüfe die in den einzelnen Merkmalen beschriebenen Berechtigungspfade und entferne alle unnötigen Rechte.

Gemäß den üblichen Sicherheitsprinzipien gewähren Sie geringste Rechte, indem Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Ersetzen Sie allgemeine Richtlinien durch spezifische Richtlinien, die nur die spezifischen Aktionen und Ressourcen gewähren, die benötigt werden. Verwenden Sie IAM Access Analyzer, um Empfehlungen auf der Grundlage des Zugriffsverlaufs zu generieren, um ungenutzte zu entfernende Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Ergebnisse für externen und ungenutzten Zugriff und Anwenden von Berechtigungen mit den geringsten Rechten im IAM-Benutzerhandbuch.

Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

Der zugehörige Principal kann einer Rechenressource, die bereits über erweiterte Berechtigungen verfügt, eine Rolle übergeben und Code in diese einschleusen. Auf diese Weise kann der Principal die volle Kontrolle über den Executor erlangen und alle Aktionen ausführen, die die Rolle des Executors zulässt.

Hat einen direkten politischen Eskalationspfad

Der zugehörige Principal kann die IAM-Richtlinien direkt ändern, um sich selbst zusätzliche Berechtigungen zu gewähren und so seine eigenen Rechte ohne Zwischenressourcen zu erweitern.

Hat einen Hijack-Pfad für Vertrauensrichtlinien

Der zugehörige Principal kann die Vertrauensrichtlinie einer IAM-Rolle so ändern, dass er selbst diese Rolle übernehmen kann, wodurch er die Berechtigungen der Rolle erhält.

Hat einen Pfad zur Daten-Ransomware

Der zugehörige Principal kann Daten auf eine Weise verschlüsseln oder löschen, die für Ransomware verwendet werden könnte, z. B. durch Verschlüsseln von Amazon S3 S3-Objekten

mit einem vom Kunden verwalteten AWS KMS Schlüssel und anschließendes Ändern der Schlüsselrichtlinie.

Hat den Beschränkungspfad entfernt

Der zugehörige Prinzipal kann Sicherheitseinschränkungen wie Zugriffsgrenzen, Dienststeuerungsrichtlinien oder ressourcenbasierte Policy-Deny-Statements aufheben und so die Möglichkeiten anderer Prinzipale oder der Ressource selbst erweitern.

Hat die Rolle bestanden, den Executor-Pfad erstellen

Der zugehörige Principal kann eine neue Rechenressource (z. B. eine Lambda-Funktion oder eine Amazon EC2 EC2-Instance) erstellen und ihr eine privilegierte Rolle zuweisen, wodurch seine eigenen Berechtigungen durch die neue Ressource effektiv gewaschen werden.

Hat einen bestehenden Executor-Pfad für die Swap-Rolle

Der zugehörige Principal kann die einer vorhandenen Rechenressource zugeordnete IAM-Rolle ändern und sie durch eine privilegiertere Rolle ersetzen, um den Zugriff zu eskalieren.

Hat einen Eskalationspfad für die Rollenkette

Der zugeordnete Principal kann eine Abfolge von Rollen übernehmen, wobei jede Rolle in der Kette über immer umfangreichere Berechtigungen verfügt, sodass letztendlich eine Rolle mit hohen Rechten erreicht wird.

Hat einen privilegierten Executor-Pfad für Inject-Code

Der zugehörige Principal kann Code in eine laufende Rechenressource mit erhöhten Rechten einfügen und dabei beliebige Operationen unter der privilegierten Rolle dieser Ressource ausführen.

Hat den Audit-Trail-Pfad deaktiviert

Der zugehörige Principal kann die Protokollierungs- oder Überwachungsdienste deaktivieren CloudTrail, um beispielsweise während oder nach einer Eskalation effektiv seine Spuren zu verwischen.

Hat Zugriff auf den vorhandenen Executor-Pfad

Der zugehörige Principal kann eine bestehende Rechenressource aufrufen oder eine Verbindung zu ihr herstellen und die ihr zugeordnete Rolle verwenden, um privilegierte Aktionen auszuführen.

Hat einen Pfad zum Minting von Anmeldeinformationen

Der zugehörige Prinzipal kann neue langfristige Anmeldeinformationen (wie Zugriffsschlüssel oder Anmeldeprofile) für andere Prinzipale erstellen und so persistente Zugriffspfade einrichten, die Passwortrotationen oder Sitzungsablaufzeiten überstehen.

Hat den Datenzugriffspfad bestanden

Der zugehörige Principal kann eine Dienstressource erstellen und ihr eine Rolle zuweisen, die Zugriff auf vertrauliche Daten hat, sodass er über die neue Ressource indirekt auf diese Daten zugreifen kann.

Hat den Pfad zur Übernahme der Rolle, der Aufgabe

Der zugehörige Principal kann eine Rolle an eine geplante oder ereignisgesteuerte Aufgabe übergeben (z. B. eine Lambda-Funktion, die durch ein Ereignis ausgelöst wird), sodass er beliebigen Code mit den Berechtigungen dieser Rolle ausführen kann.

Hat einen Single-Hop-Datenzugriffspfad

Der zugehörige Principal kann über seine vorhandenen Berechtigungen direkt auf vertrauliche Datenressourcen (wie Amazon S3 S3-Buckets oder DynamoDB-Tabellen) zugreifen, ohne dass zwischengeschaltete Eskalationsschritte erforderlich sind.

Hat einen Pfad zur Weiterentwicklung der Fähigkeiten

Der zugeordnete Principal verfügt über einen Pfad zur Eskalation von Rechten, der seine allgemeinen Fähigkeiten über das hinaus erweitert, was seine direkt zugewiesenen Berechtigungen vermuten lassen würden. Dies ist eine allgemeine Klassifizierung für Pfade, die keinem spezifischeren Muster entsprechen.

Geschäftliche Kritikalität

Die geschäftliche Wichtigkeit der Primärressource, die entweder durch Automatisierungsregeln oder durch Inferenz aus dem Namen und den Tags festgelegt wird.

Behebung von Risiken für Amazon RDS-Instances und -Cluster

AWS Security Hub kann Risikenergebnisse für Amazon RDS-Instances und -Cluster generieren.

Auf der Security Hub-Konsole werden die Amazon RDS-Instance oder der Amazon RDS-Cluster, die bzw. der an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen

im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema enthaltenen Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Ressourcen. AWS

Inhalt

- Merkmale bei der Fehlkonfiguration von Amazon RDS-Instances und -Clustern
  - Die Amazon RDS-DB-Instance ist mit öffentlichem Zugriff konfiguriert
  - Der Amazon RDS-DB-Cluster verfügt über einen Snapshot, der öffentlich geteilt wird
  - Die Amazon RDS-DB-Instance hat einen Snapshot, der öffentlich geteilt wird
  - Die Amazon RDS-DB-Instance hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist
  - Der Amazon RDS-DB-Cluster verfügt über einen Snapshot, der im Ruhezustand nicht verschlüsselt ist
  - Die Amazon RDS DB-Instance hat eine offene Sicherheitsgruppe
  - Für die Amazon RDS-DB-Instance ist die IAM-Datenbankauthentifizierung deaktiviert
  - Die Amazon RDS-DB-Instance verwendet den Standard-Admin-Benutzernamen
  - Der Amazon RDS-DB-Cluster verwendet den Standard-Admin-Benutzernamen
  - Für die Amazon RDS-DB-Instance sind automatische Nebenversions-Upgrades deaktiviert
  - Für die Amazon RDS DB-Instance sind automatische Backups deaktiviert
  - Für die Amazon RDS-DB-Instance ist der Löschschutz deaktiviert

- Für den Amazon RDS-DB-Cluster ist der Löschschutz deaktiviert
- Die Amazon RDS-DB-Instance verwendet den Standard-Port für die Datenbank-Engine
- Die Amazon RDS-DB-Instance ist nicht durch einen Backup-Plan abgedeckt

- Vertrauliche Datenmerkmale für Amazon RDS-DB-Instances
  - Die Amazon RDS-DB-Instance enthält vertrauliche Daten

Merkmale bei der Fehlkonfiguration von Amazon RDS-Instances und -Clustern

Im Folgenden werden die Merkmale einer Fehlkonfiguration und die Schritte zur Behebung von Amazon RDS-Instances und -Clustern beschrieben.

Die Amazon RDS-DB-Instance ist mit öffentlichem Zugriff konfiguriert

Amazon RDS-Instances mit öffentlichem Zugang sind potenziell über ihre Endpunkte über das Internet zugänglich. Obwohl manchmal öffentlicher Zugriff für Instance-Funktionen erforderlich ist, kann diese Konfiguration als potenzieller Angriffsvektor für unbefugte Benutzer verwendet werden, um auf Ihre Datenbank zuzugreifen. Öffentlich zugängliche Datenbanken können Port-Scans, Brute-Force-Angriffen und Ausnutzungsversuchen ausgesetzt sein. Halten Sie sich an die üblichen Sicherheitsprinzipien und beschränken Sie die Offenlegung Ihrer Datenbankressourcen durch die Öffentlichkeit.

Problembehebung: Ändern Sie die Einstellungen für den öffentlichen Zugriff

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Prüfen Sie anhand Ihrer Anwendungsarchitektur, ob die DB-Instance öffentlich zugänglich sein muss. Weitere Informationen finden Sie unter Einrichten des öffentlichen oder privaten Zugriffs in Amazon RDS.

Der Amazon RDS-DB-Cluster verfügt über einen Snapshot, der öffentlich geteilt wird

Auf öffentliche Snapshots kann jeder zugreifen AWS-Konto, wodurch vertrauliche Daten möglicherweise unbefugten Benutzern zugänglich gemacht werden. Jeder AWS-Konto hat die Erlaubnis, diese öffentlichen Snapshots zu kopieren und daraus DB-Instances zu erstellen, was zu Datenschutzverletzungen oder unberechtigtem Datenzugriff führen kann. Beschränken Sie den Zugriff auf Ihre Amazon RDS-Snapshots gemäß den bewährten Sicherheitsmethoden nur auf vertrauenswürdige AWS-Konten Organisationen und Organisationen.

Abhilfe: Konfigurieren Sie einen Amazon RDS-Snapshot für den privaten Zugriff

Öffnen Sie in der Risikoanalyse die Ressource über den Hyperlink. Informationen zum Ändern der Einstellungen für das Teilen von Snapshots finden Sie unter Teilen eines Snapshots im Amazon Aurora-Benutzerhandbuch. Informationen darüber, wie Sie das Teilen von Snapshots beenden, finden Sie unter Stoppen der Snapshot-Freigabe im Amazon Aurora-Benutzerhandbuch. .

Die Amazon RDS-DB-Instance hat einen Snapshot, der öffentlich geteilt wird

Auf öffentliche Snapshots kann jeder zugreifen AWS-Konto, wodurch vertrauliche Daten möglicherweise unbefugten Benutzern zugänglich gemacht werden. Jeder AWS-Konto hat die Erlaubnis, diese öffentlichen Snapshots zu kopieren und daraus DB-Instances zu erstellen, was zu Datenschutzverletzungen oder unberechtigtem Datenzugriff führen kann. Beschränken Sie den Zugriff auf Ihre Amazon RDS-Snapshots gemäß den bewährten Sicherheitsmethoden nur auf vertrauenswürdige AWS-Konten Organisationen und Organisationen.

Abhilfe: Konfigurieren Sie einen Amazon RDS-Snapshot für den privaten Zugriff

Öffnen Sie in der Risikoanalyse die Ressource über den Hyperlink. Informationen zum Ändern der Einstellungen für die gemeinsame Nutzung von Snapshots finden Sie unter Teilen eines DB-Snapshots im Amazon RDS-Benutzerhandbuch. Informationen darüber, wie Sie das Teilen von Snapshots beenden, finden Sie unter Beenden der gemeinsamen Nutzung eines DB-Snapshots im Amazon RDS-Benutzerhandbuch. .

Die Amazon RDS-DB-Instance hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist

Unverschlüsselte Amazon RDS-DB-Instance-Snapshots können sensible Daten preisgeben, wenn unbefugter Zugriff auf die Speicherebene erlangt wird. Ohne Verschlüsselung könnten Daten in Snapshots potenziell durch unbefugten Zugriff offengelegt werden. Dies birgt das Risiko von Datenschutz- und Compliance-Verstößen. Verschlüsseln Sie alle Datenbankressourcen und ihre Backups gemäß den bewährten Sicherheitsmethoden, um die Vertraulichkeit der Daten zu gewährleisten.

Problembehebung: Aktualisieren Sie die betroffenen Ressourcen

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird der betroffene Snapshot in der Amazon RDS-Konsole geöffnet. Sie können einen vorhandenen unverschlüsselten Snapshot nicht direkt verschlüsseln.

Erstellen Sie stattdessen eine verschlüsselte Kopie des unverschlüsselten Snapshots. Eine ausführliche Anleitung finden Sie unter Kopieren und Verschlüsseln von Amazon RDS-Ressourcen von DB-Cluster-Snapshots im Amazon Aurora-Benutzerhandbuch.

Der Amazon RDS-DB-Cluster verfügt über einen Snapshot, der im Ruhezustand nicht verschlüsselt ist

Unverschlüsselte Amazon RDS-DB-Cluster-Snapshots können sensible Daten preisgeben, wenn unbefugter Zugriff auf die Speicherebene erlangt wird. Ohne Verschlüsselung könnten Daten in Snapshots potenziell durch unbefugten Zugriff offengelegt werden. Dies birgt das Risiko von Datenschutz- und Compliance-Verstößen. Verschlüsseln Sie alle Datenbankressourcen und ihre Backups gemäß den bewährten Sicherheitsmethoden, um die Vertraulichkeit der Daten zu gewährleisten.

Problembehebung: Erstellen Sie eine verschlüsselte Kopie des Snapshots

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird der betroffene Snapshot in der Amazon RDS-Konsole geöffnet. Sie können einen vorhandenen unverschlüsselten Snapshot nicht direkt verschlüsseln.

Erstellen Sie stattdessen eine verschlüsselte Kopie des unverschlüsselten Snapshots. Eine ausführliche Anleitung finden Sie unter Kopieren und Verschlüsseln von Amazon RDS-Ressourcen von DB-Cluster-Snapshots im Amazon Aurora-Benutzerhandbuch.

Die Amazon RDS DB-Instance hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Amazon RDS-Instances zur Steuerung des eingehenden und ausgehenden Datenverkehrs. Offene Sicherheitsgruppen, die uneingeschränkten Zugriff von jeder IP-Adresse aus ermöglichen, können Ihre Datenbank-Instances unbefugtem Zugriff und potenziellen Angriffen aussetzen. Beschränken Sie gemäß den Standardsicherheitsprinzipien den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports, um das Prinzip der geringsten Rechte aufrechtzuerhalten.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen Sie die Regeln für Sicherheitsgruppen und bewerten Sie die aktuelle Konfiguration

Öffnen Sie in der Risikoanalyse die Ressource für die DB-Instance-Sicherheitsgruppe. Prüfen Sie, welche Ports geöffnet sind und über weite IP-Bereiche zugänglich sind, z. `(0.0.0.0/0 or ::/0)` B. Informationen zum Anzeigen von Sicherheitsgruppendetails finden Sie DescribeSecurityGroups in der Amazon Elastic Compute Cloud API-Referenz.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Erwägen Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken. Informationen zum Ändern von Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon EC2-Benutzerhandbuch. Informationen zum Ändern des Standardports einer vorhandenen Amazon RDS-Datenbank-Instance finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora-Benutzerhandbuch.

Für die Amazon RDS-DB-Instance ist die IAM-Datenbankauthentifizierung deaktiviert

Die IAM-Datenbankauthentifizierung ermöglicht es Ihnen, sich bei Ihrer Amazon RDS-Datenbank mit IAM-Anmeldeinformationen anstelle von Datenbankkennwörtern zu authentifizieren. Dies bietet mehrere Sicherheitsvorteile, wie z. B. eine zentrale Zugriffsverwaltung, temporäre Anmeldeinformationen und die Tatsache, dass das Speichern von Datenbankkennwörtern im Anwendungscode entfällt. Die IAM-Datenbankauthentifizierung ermöglicht die Authentifizierung bei Datenbankinstanzen mit einem Authentifizierungstoken anstelle eines Kennworts. Daher wird der Netzwerkverkehr zur und von der Datenbankinstanz mit SSL verschlüsselt. Ohne IAM-Authentifizierung verlassen sich Datenbanken in der Regel auf eine kennwortbasierte Authentifizierung, was zur Wiederverwendung von Passwörtern und schwachen Passwörtern führen kann. Aktivieren Sie die IAM-Datenbankauthentifizierung gemäß den bewährten Sicherheitsmethoden.

Problembehebung: Aktivieren Sie die IAM-Datenbankauthentifizierung

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Sie können die IAM-Datenbankauthentifizierung in den Datenbankoptionen aktivieren.

Weitere Informationen finden Sie unter Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung im Amazon RDS-Benutzerhandbuch. Nachdem Sie die IAM-Authentifizierung aktiviert haben, aktualisieren Sie Ihre DB-Instances so, dass sie die IAM-Authentifizierung anstelle der kennwortbasierten Authentifizierung verwenden.

Die Amazon RDS-DB-Instance verwendet den Standard-Admin-Benutzernamen

Die Verwendung von Standardbenutzernamen (z. B. „admin“, „root“) für DB-Instances erhöht das Sicherheitsrisiko, da diese weithin bekannt sind und häufig als Ziel von Brute-Force-Angriffen

eingesetzt werden. Standardbenutzernamen sind vorhersehbar und erleichtern es unbefugten Benutzern, Zugriff auf Ihre Datenbank zu erhalten. Bei Standardbenutzernamen müssen sich Angreifer nur Passwörter beschaffen und nicht beide, um Zugriff auf Ihre Datenbank zu erhalten. Verwenden Sie gemäß den bewährten Sicherheitsmethoden eindeutige Administrator-Benutzernamen für Ihre Datenbank-Instance, um die Sicherheit durch Undurchsichtigkeit zu erhöhen und das Risiko unberechtigter Zugriffsversuche zu verringern.

Problembehebung: Konfigurieren Sie einen eindeutigen Administrator-Benutzernamen

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Sie können den Administrator-Benutzernamen einer vorhandenen Amazon RDS-DB-Instance nicht ändern. Um einen eindeutigen Administratornamen zu erstellen, müssen Sie eine neue DB-Instance mit einem benutzerdefinierten Benutzernamen erstellen und Ihre Daten migrieren.

Der Amazon RDS-DB-Cluster verwendet den Standard-Admin-Benutzernamen

Die Verwendung von Standardbenutzernamen (z. B. „admin“, „root“) für DB-Instances erhöht das Sicherheitsrisiko, da diese weithin bekannt sind und häufig als Ziel von Brute-Force-Angriffen eingesetzt werden. Standardbenutzernamen sind vorhersehbar und erleichtern es unbefugten Benutzern, Zugriff auf Ihre Datenbank zu erhalten. Bei Standardbenutzernamen müssen sich Angreifer nur Passwörter beschaffen und nicht beide, um Zugriff auf Ihre Datenbank zu erhalten. Verwenden Sie gemäß den bewährten Sicherheitsmethoden eindeutige Administrator-Benutzernamen für Ihre Datenbank-Instance, um die Sicherheit durch Undurchsichtigkeit zu erhöhen und das Risiko unberechtigter Zugriffsversuche zu verringern.

Problembehebung: Konfigurieren Sie einen eindeutigen Administrator-Benutzernamen

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Sie können den Administrator-Benutzernamen einer vorhandenen Amazon RDS-DB-Instance nicht ändern. Um einen eindeutigen Administratornamen zu erstellen, müssen Sie eine neue DB-Instance mit einem benutzerdefinierten Benutzernamen erstellen und Ihre Daten migrieren.

Für die Amazon RDS-DB-Instance sind automatische Nebenversions-Upgrades deaktiviert

Automatische Nebenversions-Upgrades stellen sicher, dass Ihre Amazon RDS-Instances automatisch kleinere Engine-Versions-Upgrades erhalten, sobald diese verfügbar sind. Diese Upgrades beinhalten häufig wichtige Sicherheitspatches und Bugfixes, die dazu beitragen, die

Sicherheit und Stabilität Ihrer Datenbank aufrechtzuerhalten. Es besteht die Gefahr, dass Ihre Datenbank mit bekannten Sicherheitslücken läuft, die in neueren Nebenversionen behoben wurden. Ohne automatische Updates können sich bei Datenbankinstanzen Sicherheitslücken anhäufen, wenn neue CVEs entdeckt werden. Aktivieren Sie gemäß den bewährten Sicherheitsmethoden automatische Nebenversions-Upgrades für alle Amazon RDS-Instances.

Problembehebung: Aktivieren Sie automatische Upgrades für Nebenversionen

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Sie können die Einstellungen für automatische kleinere Upgrades auf der Registerkarte Wartung und Backups einsehen.

Weitere Informationen finden Sie unter Automatische Upgrades von Nebenversionen für Amazon RDS for MySQL. Sie können Ihr Wartungsfenster auch so konfigurieren, dass es in Zeiten niedriger Datenbankaktivität stattfindet.

Für die Amazon RDS DB-Instance sind automatische Backups deaktiviert

Automatisierte Backups ermöglichen eine zeitpunktgenaue Wiederherstellung Ihrer Amazon RDS-Instances, sodass Sie Ihre Datenbank zu einem beliebigen Zeitpunkt innerhalb Ihres Aufbewahrungszeitraums wiederherstellen können. Wenn automatische Backups deaktiviert sind, riskieren Sie den Verlust von Daten im Falle einer böswilligen Löschung, Datenbeschädigung oder anderen Datenverlust-Szenarien. Bei böswilligen Aktivitäten wie Ransomware-Angriffen, dem Löschen oder einer Beschädigung von Datenbanktabellen reduziert die Möglichkeit, die Wiederherstellung auf einen Zeitpunkt vor dem Vorfall durchzuführen, die Zeit, die für die Wiederherstellung nach einem Vorfall erforderlich ist. Ermöglichen Sie automatische Backups mit einer angemessenen Aufbewahrungsfrist für alle Produktionsdatenbanken, indem Sie den bewährten Sicherheitsmethoden folgen.

Für die Amazon RDS-DB-Instance ist der Löschschutz deaktiviert

Der Schutz vor dem Löschen von Datenbanken ist eine Funktion, die dazu beiträgt, das Löschen Ihrer Datenbank-Instances zu verhindern. Wenn der Löschschutz deaktiviert ist, kann Ihre Datenbank von jedem Benutzer mit ausreichenden Berechtigungen gelöscht werden, was möglicherweise zu Datenverlust oder Anwendungsausfällen führen kann. Angreifer können Ihre Datenbank löschen, was zu Betriebsunterbrechungen, Datenverlust und einer längeren Wiederherstellungszeit führt. Aktivieren Sie gemäß den bewährten Sicherheitsmethoden den Löschschutz für Ihre RDS-DB-Instances, um ein böswilliges Löschen zu verhindern.

Behebung: Aktivieren Sie den Löschschutz für Ihren Amazon RDS-DB-Cluster

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird der betroffene DB-Cluster geöffnet.

Für den Amazon RDS-DB-Cluster ist der Löschschutz deaktiviert

Der Schutz vor dem Löschen von Datenbanken ist eine Funktion, die dazu beiträgt, das Löschen Ihrer Datenbank-Instances zu verhindern. Wenn der Löschschutz deaktiviert ist, kann Ihre Datenbank von jedem Benutzer mit ausreichenden Berechtigungen gelöscht werden, was möglicherweise zu Datenverlust oder Anwendungsausfällen führen kann. Angreifer können Ihre Datenbank löschen, was zu Betriebsunterbrechungen, Datenverlust und einer längeren Wiederherstellungszeit führt. Aktivieren Sie gemäß den bewährten Sicherheitsmethoden den Löschschutz für Ihre RDS-DB-Cluster, um böswilliges Löschen zu verhindern.

Behebung: Aktivieren Sie den Löschschutz für Ihren Amazon RDS-DB-Cluster

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird der betroffene DB-Cluster geöffnet.

Die Amazon RDS-DB-Instance verwendet den Standard-Port für die Datenbank-Engine

Amazon RDS-Instances, die Standard-Ports für Datenbank-Engines verwenden, können erhöhten Sicherheitsrisiken ausgesetzt sein, da diese Standard-Ports weithin bekannt sind und häufig von automatisierten Scan-Tools angegriffen werden. Wenn Sie Ihre DB-Instance so ändern, dass sie nicht standardmäßige Ports verwendet, wird eine zusätzliche Sicherheitsebene durch Unklarheit hinzugefügt. Dadurch wird es für nicht autorisierte Benutzer schwieriger, automatische oder gezielte Angriffe auf Ihre Datenbank durchzuführen. Standard-Ports werden in der Regel von Unbefugten durchsucht und können dazu führen, dass Ihre DB-Instance ins Visier genommen wird. Ändern Sie den Standard-Port gemäß den bewährten Sicherheitsmethoden in einen benutzerdefinierten Port, um das Risiko automatisierter oder gezielter Angriffe zu verringern.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Aktualisieren Sie die betroffenen Ressourcen

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet.

Aktualisieren Sie die Verbindungszeichenfolgen der Anwendung

Nachdem Sie den Port geändert haben, aktualisieren Sie alle Anwendungen und Dienste, die eine Verbindung zu Ihrer Amazon RDS-Instance herstellen, sodass sie die neue Portnummer verwenden.

Die Amazon RDS-DB-Instance ist nicht durch einen Backup-Plan abgedeckt

AWS Backup ist ein vollständig verwalteter Backup-Service, der die Sicherung von Daten auf allen Ebenen zentralisiert und automatisiert. AWS-Services Wenn Ihre DB-Instance nicht durch einen Backup-Plan abgedeckt ist, riskieren Sie den Verlust von Daten im Falle einer böswilligen Löschung, Datenbeschädigung oder anderen Datenverlust-Szenarien. Bei böswilligen Aktivitäten wie Ransomware-Angriffen, dem Löschen von Datenbanktabellen oder einer Beschädigung von Datenbanktabellen reduziert die Möglichkeit, die Wiederherstellung auf einen Zeitpunkt vor dem Vorfall durchzuführen, die Zeit, die für die Wiederherstellung nach einem Vorfall erforderlich ist. Nehmen Sie Ihre Amazon RDS-Instances gemäß den bewährten Sicherheitsmethoden in einen Backup-Plan auf, um den Datenschutz zu gewährleisten.

Problembehebung: Erstellen Sie einen Backup-Plan für Ihre DB-Instance und weisen Sie ihn zu

Wählen Sie in der Risikoanalyse den Link zur Ressource aus. Dadurch wird die betroffene DB-Instance in der Amazon RDS-Konsole geöffnet. Überlegen Sie, welche Backup-Frequenz, Aufbewahrungsdauer und Lebenszyklusregeln für Ihre Anwendungen am besten geeignet sind.

Vertrauliche Datenmerkmale für Amazon RDS-DB-Instances

Im Folgenden finden Sie die Merkmale vertraulicher Daten für Amazon RDS-DB-Instances und empfohlene Abhilfemaßnahmen.

Die Amazon RDS-DB-Instance enthält vertrauliche Daten

Ein Datensicherheitsscan hat bestätigt, dass vertrauliche Datensätze in der Amazon RDS-DB-Instance vorhanden sind. Ein integriertes Datensicherheitsprodukt legt dieses Merkmal fest, wenn es den Inhalt der DB-Instance überprüft und Datensätze identifiziert, die geschützt werden müssen.

Das Vorhandensein sensibler Daten erhöht die Auswirkungen jeder anderen Schwachstelle auf derselben DB-Instance. Ein Netzwerkpfad oder eine Konfiguration mit erlaubtem Zugriff, die andernfalls Anwendungsdaten preisgeben würde, führt stattdessen zu regulierten oder vertraulichen Datensätzen. Ein Bedrohungsakteur, der die DB-Instance erreicht, kann diese Datensätze in großen Mengen abfragen, kopieren und außerhalb Ihrer Umgebung aufbewahren. Der Bedrohungsakteur kann auch alle wiederhergestellten Anmeldeinformationen verwenden, um sich bei anderen Systemen zu authentifizieren. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den

Netzwerk- und Identitätszugriff auf Amazon RDS-DB-Instances, die vertrauliche Datensätze speichern, einzuschränken und diese Datensätze im Ruhezustand und bei der Übertragung zu verschlüsseln.

Zu den sensiblen Daten können gehören:

- Anmeldeinformationen — wie Passwörter, Zugangsschlüssel und Verbindungszeichenfolgen
- Persönlich identifizierbare Informationen
- Finanzinformationen — wie Kontonummern und Zahlungskartendaten
- Vertrauliche Inhalte, die geschützt werden müssen

Das Entfernen der vertraulichen Aufzeichnungen ist die einzige Möglichkeit, dieses Merkmal zu löschen. Wenn Ihre Arbeitslast erfordert, dass die DB-Instance vertrauliche Daten speichert, reduzieren die folgenden bewährten Sicherheitsmethoden das Risiko einer Gefährdung.

Überprüfen Sie die sensiblen Daten auf der DB-Instance

Öffnen Sie in der Risikoanalyse die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Notieren Sie sich die DB-Instance-ID und notieren Sie sich die VPC-Sicherheitsgruppen, die unter Konnektivität und Sicherheit aufgeführt sind. Überprüfen Sie das Ergebnis zur Datensicherheit, das die vertraulichen Datensätze gemeldet hat, um festzustellen, in welchen Datenbanken, Schemas und Tabellen sie enthalten sind.

Implementieren Sie je nach Art der erkannten vertraulichen Daten die entsprechenden Sicherheitskontrollen:

- Beschränken Sie den eingehenden Netzwerkzugriff — Wählen Sie in der Amazon RDS-Konsole Datenbanken, wählen Sie die DB-Instance und anschließend Connectivity & Security aus. Öffnen Sie jede angehängte VPC-Sicherheitsgruppe und überprüfen Sie ihre Regeln für eingehenden Datenverkehr. Ersetzen Sie alle Regeln, die den Datenbankport von `0.0.0.0/0` oder `::/0` aus den spezifischen CIDR-Bereichen oder Sicherheitsgruppen-IDs zulassen, die Ihre Anwendungen verwenden. Weitere Informationen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Benutzerhandbuch für Amazon RDS.
- Öffentliche Zugänglichkeit entfernen — Wählen Sie in der Amazon RDS-Konsole die DB-Instance aus, wählen Sie Ändern und setzen Sie unter Konnektivität den öffentlichen Zugriff auf Nicht öffentlich zugänglich. Platzieren Sie die DB-Instance in privaten Subnetzen, die keine Route zu einem Internet-Gateway haben. Erreichen Sie sie von Ihren Anwendungen aus über die VPC,

AWS Direct Connect oder eine VPN-Verbindung. Weitere Informationen finden Sie unter Working with a DB instance in a VPC (Arbeiten mit einer DB-Instance in einer VPC) im Amazon-RDS-Benutzerhandbuch.

- Beschränken Sie, wer sich bei der Datenbank authentifizieren kann — Gewähren Sie jeder Anwendung und jedem Benutzer nur die Datenbankberechtigungen, die für ihre Funktion erforderlich sind. Widerrufen Sie allen Datenbankbenutzern, die ihn nicht benötigen, den Lesezugriff auf die Tabellen, die vertrauliche Datensätze enthalten. Verwenden Sie die IAM-Datenbankauthentifizierung, damit IAM-Identitäten und kurzlebige Token den Zugriff statt langlebiger Datenbankkennwörter kontrollieren. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung im Amazon RDS-Benutzerhandbuch.
- Verschlüsseln Sie die vertraulichen Datensätze im Ruhezustand — Wählen Sie in der Amazon RDS-Konsole die DB-Instance aus und klicken Sie auf den Tab Configuration, um zu sehen, ob die DB-Instance Verschlüsselung verwendet. Sie können die Verschlüsselung im Ruhezustand auf einer vorhandenen unverschlüsselten DB-Instance nicht aktivieren. Um ihre Daten zu verschlüsseln, erstellen Sie einen Snapshot der DB-Instance. Kopieren Sie den Snapshot und wählen Sie einen AWS KMS-Schlüssel für die Kopie aus. Stellen Sie dann die verschlüsselte Snapshot-Kopie in einer neuen DB-Instance wieder her. Verweisen Sie Ihre Anwendungen erneut auf den neuen Endpunkt und löschen Sie die unverschlüsselte DB-Instance und ihre Snapshots. Weitere Informationen finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.
- Verschlüsselung während der Übertragung erforderlich — Konfigurieren Sie Ihre Datenbank-Clients so, dass sie SSL/TLS mithilfe des Amazon RDS-Zertifikatspakets eine Verbindung herstellen. Erzwingen Sie verschlüsselte Verbindungen auf der DB-Instance mithilfe des Parameters, den Ihre Datenbank-Engine für diesen Zweck bereitstellt. Weitere Informationen finden Sie unter SSL/TLS Zum Verschlüsseln einer Verbindung zu einer DB-Instance oder einem Cluster verwenden im Amazon RDS-Benutzerhandbuch.
- Überwachen Sie den Zugriff auf die DB-Instance — Veröffentlichen Sie die CloudWatch Datenbank-Engine-Protokolle in Amazon Logs und überprüfen Sie sie auf Verbindungen aus unerwarteten Quellen und auf Abfragen von Tabellen, die vertrauliche Datensätze enthalten. Weitere Informationen finden Sie unter Überwachen von Amazon RDS-Protokolldateien im Amazon RDS-Benutzerhandbuch.

Behebung von Risiken für Amazon S3-Buckets

AWS Security Hub kann Risikoprüfungen für Amazon Simple Storage Service (Amazon S3) -Buckets generieren.

Auf der Security Hub-Konsole werden der Amazon S3-Bucket, der an einer Gefahrenfeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Erkennungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema enthaltenen Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Ressourcen. AWS

Inhalt

- Merkmale bei der Fehlkonfiguration von Amazon S3-Buckets
  - Für den Amazon S3-Bucket ist die Versionierung deaktiviert
  - Im Amazon S3-Bucket ist Object Lock deaktiviert
  - Der Amazon S3-Bucket ist im Ruhezustand nicht verschlüsselt mit AWS KMS keys
  - Multi-factor Das Löschen durch Authentifizierung (MFA) ist in einem versionierten Amazon S3-Bucket deaktiviert
  - Der Amazon S3-Bucket ermöglicht Principals von anderen AWS Konten zum Ändern von Bucket-Berechtigungen
- Erreichbarkeitsmerkmale für Amazon S3-Buckets
  - Der Amazon S3-Bucket hat öffentlichen Lesezugriff
  - Der Amazon S3-Bucket hat öffentlichen Schreibzugriff
- Vertrauliche Datenmerkmale für Amazon S3-Buckets
  - Der Amazon S3-Bucket enthält vertrauliche Daten

Merkmale bei der Fehlkonfiguration von Amazon S3-Buckets

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Amazon S3-Buckets und empfohlene Abhilfemaßnahmen.

Für den Amazon S3-Bucket ist die Versionierung deaktiviert

Die Amazon S3-Versionierung hilft Ihnen dabei, mehrere Varianten eines Objekts im selben Bucket zu speichern. Wenn die Versionierung deaktiviert ist, speichert Amazon S3 nur die neueste Version jedes Objekts. Das bedeutet, dass Objekte, die versehentlich oder in böswilliger Absicht gelöscht oder überschrieben werden, nicht wiederhergestellt werden können. Versioning-enabled Buckets bieten Schutz vor versehentlichem Löschen, Anwendungsausfällen und Sicherheitsvorfällen wie Ransomware-Angriffen, bei denen Daten unbefugt geändert oder gelöscht werden könnten. Halten Sie sich an die bewährten Sicherheitsmethoden und aktivieren Sie die Versionierung für Buckets, die wichtige Daten enthalten, die bei Verlust nur schwer oder gar nicht wiederhergestellt werden könnten.

Problembehebung: Aktivieren Sie die Versionierung

Informationen zum Aktivieren der Amazon S3-Versionierung für einen Bucket finden Sie unter Enabling versioning on buckets im Amazon S3-Benutzerhandbuch. Wenn Sie die Versionierung aktivieren, sollten Sie in Betracht ziehen, Lebenszyklusregeln zur Speicherverwaltung zu implementieren, da bei der Versionierung mehrere Kopien von Objekten verwaltet werden.

Im Amazon S3-Bucket ist Object Lock deaktiviert

Amazon S3 Object Lock bietet ein WORM-Modell (Write-Once-Read-Many) für Amazon S3-Objekte, das verhindert, dass diese für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben werden. Wenn Object Lock deaktiviert ist, könnten Ihre Objekte anfällig für versehentliches oder böswilliges Löschen, Ändern oder Verschlüsseln durch Ransomware sein. Object Lock ist besonders wichtig für die Einhaltung gesetzlicher Anforderungen, die eine unveränderliche Datenspeicherung erfordern, und für den Schutz vor raffinierten Bedrohungen wie Ransomware, die versuchen könnte, Ihre Daten zu verschlüsseln. Durch die Aktivierung von Object Lock können Sie Aufbewahrungsrichtlinien als zusätzliche Datenschutzebene durchsetzen und eine unveränderliche Backup-Strategie für Ihre wichtigen Daten erstellen. Aktivieren Sie Object Lock gemäß den bewährten Sicherheitsmethoden, um böswillige Änderungen an Ihren Objekten zu verhindern.

Behebung: Konfigurieren Sie S3 Object Lock

Beachten Sie, dass Object Lock nur aktiviert werden kann, wenn Sie einen neuen Bucket erstellen. Sie müssen also einen neuen Bucket mit aktivierter Objektsperre erstellen. Bei großen Migrationen

sollten Sie erwägen, Batch Operations zu verwenden, um Objekte in den neuen Bucket zu kopieren. Bevor Sie Objekte sperren, müssen Sie auch Amazon S3 Versioning und Object Lock für einen Bucket aktivieren. Da Object Lock nur für neue Buckets aktiviert werden kann, müssen Sie vorhandene Daten in einen neuen Bucket migrieren, in dem Object Lock aktiviert ist. Informationen zur Konfiguration von Object Lock für einen Bucket finden Sie unter Configuring Amazon S3 Object Lock im Amazon S3-Benutzerhandbuch. Wählen Sie nach der Einrichtung von Object Lock einen geeigneten Aufbewahrungsmodus, der Ihrer Umgebung entspricht.

Der Amazon S3-Bucket ist im Ruhezustand nicht verschlüsselt mit AWS KMS keys

Amazon S3 wendet serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln als Standardverschlüsselungsstufe für alle neuen Buckets an. Die von Amazon S3 verwalteten Schlüssel bieten zwar einen starken Verschlüsselungsschutz, bieten jedoch nicht das gleiche Maß an Zugriffskontroll- und Überwachungsfunktionen wie AWS Key Management Service Schlüssel. Bei Verwendung von KMS-Schlüsseln sind für den Zugriff auf Objekte Berechtigungen sowohl für den Amazon S3-Bucket als auch für den KMS-Schlüssel erforderlich, mit dem das Objekt verschlüsselt wurde. Dies ist besonders wichtig für sensible Daten, bei denen Sie eine genaue Kontrolle darüber benötigen, wer auf die verschlüsselten Objekte zugreifen kann, und eine umfassende Auditprotokollierung der Verwendung von Verschlüsselungsschlüsseln benötigen. Verwenden Sie KMS-Schlüssel gemäß den bewährten Sicherheitsmethoden zum Verschlüsseln von Buckets mit vertraulichen Daten oder für Umgebungen mit strengen Compliance-Anforderungen.

Problembehebung: Konfigurieren Sie den S3-Bucket-Schlüssel

Informationen zur Konfiguration eines Buckets zur Verwendung eines Amazon S3-Bucket-Schlüssels für neue Objekte finden Sie im Amazon S3-Benutzerhandbuch unter Konfiguration Ihres Buckets zur Verwendung eines Amazon S3-Bucket-Schlüssels mit SSE-KMS für neue Objekte. Informationen zum Verschlüsseln eines vorhandenen Objekts finden Sie im AWS Storage-Blog unter Verschlüsseln von Objekten mit Amazon S3-Batchoperationen.

Beachten Sie bei der Implementierung der AWS KMS Verschlüsselung Folgendes:

- Schlüsselverwaltung — Entscheiden Sie, ob Sie einen AWS verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel (CMK) verwenden möchten. CMKs bieten Kunden die volle Kontrolle über den Lebenszyklus und die Verwendung ihrer Schlüssel. Weitere Informationen zum Unterschied zwischen diesen beiden Schlüsseltypen finden Sie unter AWS KMS-Schlüssel im AWS Key Management Service Entwicklerhandbuch.

- Schlüsselrotation — Für zusätzliche Sicherheitsmaßnahmen aktivieren Sie die automatische Schlüsselrotation für Ihre KMS-Schlüssel. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Automatische Schlüsselrotation aktivieren.

Multi-factor Das Löschen durch Authentifizierung (MFA) ist in einem versionierten Amazon S3-Bucket deaktiviert

Multi-factor Das Löschen durch Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene für Ihren Amazon S3-Bucket. Für destruktive Amazon S3-Operationen ist eine mehrstufige Authentifizierung erforderlich. Wenn das MFA-Löschen deaktiviert ist, können Benutzer mit den entsprechenden Berechtigungen Objektversionen dauerhaft löschen oder die Versionierung in Ihrem Bucket aussetzen, ohne dass zusätzliche Authentifizierungsprobleme auftreten. Die Aktivierung des MFA-Löschens schützt Sie vor unbefugtem oder versehentlichem Löschen Ihrer Daten und bietet verbesserten Schutz vor Ransomware-Angriffen, internen Bedrohungen und Betriebsfehlern. Die MFA-Löschung ist besonders nützlich für Buckets, die wichtige oder Compliance-sensible Daten enthalten, die vor unbefugtem Löschen geschützt werden müssen. Aktivieren Sie MFA für Ihre Amazon S3-Buckets gemäß den bewährten Sicherheitsmethoden.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Überprüfen Sie die MFA-Typen

AWS unterstützt die folgenden MFA-Typen. Obwohl die Authentifizierung mit einem physischen Gerät in der Regel einen höheren Sicherheitsschutz bietet, ist die Verwendung jeder Art von MFA sicherer als die Deaktivierung von MFA.

Setzen Sie MFA auf der Ebene der Ressourcenrichtlinien durch

Verwenden Sie den `aws:MultiFactorAuthAge` Bedingungsschlüssel in einer Bucket-Richtlinie, um MFA für sensible Vorgänge vorzuschreiben. Weitere Informationen finden Sie unter Erfordernis von MFA im Amazon S3-Benutzerhandbuch.

MFA aktivieren

Um das Löschen von MFA zu aktivieren, stellen Sie zunächst sicher, dass die Versionierung in Ihrem Amazon S3-Bucket aktiviert ist. Das Löschen von MFA wird nur für Buckets unterstützt, für die die Versionierung aktiviert ist. Informationen zur Aktivierung der Amazon S3-Versionierung finden

Sie unter Enabling versioning on buckets im Amazon S3-Benutzerhandbuch. Das Löschen von MFA kann nicht über die Amazon S3-Konsole aktiviert werden. Sie müssen die Amazon S3-API verwenden oder die AWS CLI. Weitere Informationen finden Sie unter Konfiguration des MFA-Löschvorgangs im Amazon S3-Benutzerhandbuch.

Der Amazon S3-Bucket ermöglicht Principals von anderen AWS Konten zum Ändern von Bucket-Berechtigungen

Amazon S3-Bucket-Richtlinien steuern den Zugriff auf Buckets und Objekte. Wenn Bucket-Richtlinien es Principals anderer AWS Konten ermöglichen, Bucket-Berechtigungen zu ändern, können nicht autorisierte Benutzer Ihren Bucket neu konfigurieren. Wenn die Anmeldeinformationen für externe Principals kompromittiert werden, können unbefugte Benutzer die Kontrolle über Ihren Bucket erlangen, was zu Datenschutzverletzungen oder Serviceunterbrechungen führt. Beschränken Sie die Aktionen zur Rechteverwaltung gemäß den Standardsicherheitsprinzipien nur auf vertrauenswürdige Principals.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen und identifizieren Sie Bucket-Richtlinien

Identifizieren Sie in der Exposure den Amazon S3-Bucket im ARN-Feld. Wählen Sie in der Amazon S3-Konsole den Bucket aus und navigieren Sie zur Registerkarte Berechtigungen, um die Bucket-Richtlinie zu überprüfen. Überprüfen Sie die dem Bucket zugeordnete Berechtigungsrichtlinie. Halten Sie Ausschau nach Richtlinienerklärungen, die ähnliche Aktionen gewähren, `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` oder nach Richtlinienerklärungen, die den Zugriff auf Principals außerhalb Ihres Accounts ermöglichen, wie in der Hauptaussage angegeben.

Ändern Sie die Bucket-Richtlinie

Ändern Sie die Bucket-Richtlinie, um Aktionen, die anderen AWS Konten gewährt wurden, zu entfernen oder einzuschränken:

- Entfernen Sie Richtlinienerklärungen, die externen Konten Aktionen zur Verwaltung von Berechtigungen gewähren.
- Wenn kontoübergreifender Zugriff erforderlich ist, ersetzen Sie allgemeine Berechtigungen (`s3:*`) durch spezifische Aktionen, die keine Bucket-Berechtigungsverwaltung beinhalten.

Informationen zum Ändern einer Bucket-Richtlinie finden Sie im Amazon S3-Benutzerhandbuch unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3-Konsole.

Erreichbarkeitsmerkmale für Amazon S3-Buckets

Im Folgenden finden Sie Erreichbarkeitsmerkmale für Amazon S3-Buckets und empfohlene Abhilfemaßnahmen.

Der Amazon S3-Bucket hat öffentlichen Lesezugriff

Amazon S3-Buckets mit öffentlichem Lesezugriff ermöglichen es jedem im Internet, den Inhalt Ihres Buckets einzusehen. Dies kann zwar für öffentlich zugängliche Websites oder gemeinsam genutzte Ressourcen erforderlich sein, kann jedoch zu Sicherheitsrisiken führen, wenn der Bucket sensible Daten enthält. Öffentlicher Lesezugriff kann zu unbefugtem Anzeigen und Herunterladen führen, was zu Datenschutzverletzungen führen kann, wenn sensible Daten in diesen Buckets gespeichert werden. Beschränken Sie den Zugriff auf Amazon S3-Buckets gemäß den Standardsicherheitsprinzipien auf die erforderlichen Benutzer und Systeme.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Blockieren Sie den öffentlichen Zugriff auf Bucket-Ebene

Amazon S3 bietet Einstellungen zum Blockieren des öffentlichen Zugriffs, die sowohl auf Bucket- als auch auf Kontoebene konfiguriert werden können, um den öffentlichen Zugriff unabhängig von Bucket-Richtlinien oder ACLs zu verhindern. Weitere Informationen finden Sie im Amazon S3-Benutzerhandbuch unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher. Nachdem Sie den öffentlichen Zugriff gesperrt haben, überprüfen Sie Ihre Bucket-Zugriffskontrollkonfiguration, um sicherzustellen, dass sie Ihren Zugriffsanforderungen entspricht. Überprüfen Sie dann Ihre Amazon S3-Bucket-Richtlinie, um explizit zu definieren, wer auf Ihren Bucket zugreifen kann. Beispiele für Bucket-Richtlinien finden Sie unter Beispiele für Amazon S3-Bucket-Richtlinien im Amazon S3-Benutzerhandbuch.

Alternative Zugangsmethoden

Wenn öffentlicher Lesezugriff erforderlich ist, sollten Sie diese sichereren Alternativen in Betracht ziehen:

- Amazon CloudFront — Verwenden Sie es CloudFront mit einer Origin Access Identity (OAI) oder Origin Access Control (OAC), um den Lesezugriff von einem privaten Amazon S3-Bucket

aus zu ermöglichen. Diese Alternative schränkt den direkten Zugriff auf Ihren Amazon S3-Bucket ein und ermöglicht gleichzeitig den öffentlichen Zugriff auf Inhalte über. CloudFront Weitere Informationen finden Sie unter Beschränken des Zugriffs auf einen Amazon S3-Ursprung im Amazon CloudFront Developer Guide.

- Vorsignierte URLs — Verwenden Sie vorsignierte URLs für den temporären Zugriff auf bestimmte Objekte. Weitere Informationen finden Sie unter Teilen von Objekten mit vorsignierten URLs im Amazon S3-Benutzerhandbuch.

Der Amazon S3-Bucket hat öffentlichen Schreibzugriff

Amazon S3-Buckets mit öffentlichem Schreibzugriff ermöglichen es jedem im Internet, Objekte in Ihrem Bucket hochzuladen, zu ändern oder zu löschen. Dies birgt erhebliche Sicherheitsrisiken, einschließlich der Möglichkeit, dass jemand bösartige Dateien hochlädt, vorhandene Dateien ändert und Daten löscht. Durch öffentlichen Schreibzugriff entstehen Sicherheitslücken, die von Angreifern ausgenutzt werden können. Beschränken Sie den Schreibzugriff auf Ihre Amazon S3-Buckets gemäß den Standardsicherheitsprinzipien auf nur die erforderlichen Benutzer und Systeme.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Sperren Sie den öffentlichen Zugriff auf Konto- und Bucket-Ebene

Amazon S3 bietet Einstellungen zum Blockieren des öffentlichen Zugriffs, die sowohl auf Bucket- als auch auf Kontoebene konfiguriert werden können, um den öffentlichen Zugriff unabhängig von Bucket-Richtlinien oder ACLs zu verhindern. Weitere Informationen finden Sie im Amazon S3-Benutzerhandbuch unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher.

Ändern Sie die Bucket-Richtlinien

Einen detaillierteren Ansatz zum Entfernen des öffentlichen Schreibzugriffs finden Sie in der Bucket-Richtlinie. Sie können nach `s3:PutObjects3:DeleteObject`, oder `s3:*` suchen. Weitere Informationen zur Verwaltung von Bucket-Richtlinien finden Sie unter Bucket-Richtlinien für Amazon S3 im Amazon S3-Benutzerhandbuch.

Alternative Zugriffsmethoden

Wenn öffentlicher Schreibzugriff erforderlich ist, sollten Sie diese sichereren Alternativen in Betracht ziehen:

- Vorsignierte URLs — Verwenden Sie vorsignierte URLs für den temporären Zugriff auf bestimmte Objekte. Weitere Informationen finden Sie unter Teilen von Objekten mit vorsignierten URLs im Amazon S3-Benutzerhandbuch.
- Amazon API Gateway-Proxy — Verwenden Sie einen Vermittler wie API Gateway mit, um Anfragen AWS Lambda zu validieren und zu autorisieren, bevor Sie sie in Ihren Amazon S3-Bucket schreiben. Dieser Ansatz stellt sicher, dass Kunden niemals direkt in den Bucket schreiben. Weitere Informationen finden Sie unter Tutorial: Erstellen Sie eine REST-API als Amazon S3-Proxy im API Gateway Developer Guide.
- Amazon CloudFront — Verwenden Sie es CloudFront mit einem Origin Access Control (OAC), das so konfiguriert ist, dass Anfragen immer signiert werden. Aktivieren Sie die PUT- und POST-Methoden, um authentifizierte Schreibvorgänge zu ermöglichen, ohne Ihren Amazon S3-Bucket direkt preiszugeben. Konfigurieren Sie Ihre Bucket-Richtlinie so, dass die `s3:DeleteObject` Berechtigungen nur autorisierten Principals vorbehalten sind, sodass nicht autorisierte Benutzer Objekte, die Sie behalten möchten, nicht löschen können. Weitere Informationen finden Sie unter Beschränken Sie den Zugriff auf einen Amazon S3-Ursprung im Amazon CloudFront Developer Guide.

Vertrauliche Datenmerkmale für Amazon S3-Buckets

Im Folgenden finden Sie die Merkmale vertraulicher Daten für Amazon S3-Buckets und empfohlene Abhilfemaßnahmen.

Der Amazon S3-Bucket enthält vertrauliche Daten

Ein Datensicherheitsscan hat bestätigt, dass sensible Daten im Amazon S3-Bucket vorhanden sind. Ein integriertes Datensicherheitsprodukt legt dieses Merkmal fest, wenn es die Objekte im Bucket untersucht und Inhalte identifiziert, die geschützt werden müssen. Security Hub meldet das Merkmal auf dieselbe Weise, unabhängig davon, welches Produkt die Inspektion durchgeführt hat.

Zu den sensiblen Daten können gehören:

- Anmeldeinformationen
- Persönlich identifizierbare Informationen
- Finanzinformationen
- Vertrauliche Inhalte, die geschützt werden müssen

Wenn sensible Daten durch Fehlkonfiguration oder unbefugten Zugriff offengelegt werden, kann dies zu Compliance-Verstößen, Datenschutzverletzungen, Identitätsdiebstahl oder finanziellen Verlusten führen. Halten Sie sich an die bewährten Sicherheitsmethoden und sorgen Sie für eine korrekte Klassifizierung der Daten und die kontinuierliche Überwachung sensibler Daten in Ihren Amazon S3-Buckets.

Abhilfe

Um dieses Merkmal zu löschen, entfernen Sie die sensiblen Daten aus dem Bucket. Wenn Ihr Workload erfordert, dass der Bucket vertrauliche Daten speichert, implementieren Sie die folgenden Sicherheitskontrollen, um das Risiko einer Offenlegung zu verringern.

Überprüfen Sie die sensiblen Daten im Bucket

Wählen Sie in der Risikoanalyse die Option Ressource öffnen aus. Prüfen Sie die Ergebnisse zur Datensicherheit, in der die vertraulichen Daten gemeldet wurden, um festzustellen, welche Objekte oder Präfixe diese enthalten. Wenn die Entdeckung von Macie stammt, beschreibt der Ergebnistyp die Kategorie der vertraulichen Daten. Weitere Informationen finden Sie im Amazon Macie-Benutzerhandbuch unter Typen von Macie-Ergebnissen.

Implementieren Sie je nach Art der entdeckten sensiblen Daten die entsprechenden Sicherheitskontrollen:

- Beschränken Sie den Zugriff auf den Bucket — Überprüfen Sie die Bucket-Berechtigungen, um sicherzustellen, dass sie dem Prinzip der geringsten Zugriffsrechte entsprechen. Verwenden Sie IAM-Richtlinien, Bucket-Richtlinien und ACLs, um den Zugriff einzuschränken. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon S3 im Amazon S3-Benutzerhandbuch.
- Serverseitige Verschlüsselung aktivieren — Aktivieren Sie die serverseitige Verschlüsselung mit KMS-Schlüsseln für zusätzlichen Schutz. Weitere Informationen finden Sie unter Verwenden der serverseitigen Verschlüsselung mit AWS KMS-Schlüsseln (SSE-KMS) im Amazon S3-Benutzerhandbuch.
- Redigieren oder transformieren Sie die vertraulichen Daten — Wenn die Objekte keine vertraulichen Werte beibehalten müssen, verwenden Sie diese Option, AWS Glue DataBrew um die Daten vorzubereiten. Wenden Sie die Maskierungs-, Ersetzungs- oder Hash-Transformationen an, mit denen diese Werte entfernt werden, bevor die nachgelagerten Systeme die Daten verarbeiten. Schreiben Sie die vorbereitete Ausgabe in einen separaten Bucket, der über eigene Zugriffskontrollen verfügt. Weitere Informationen finden Sie unter Was ist AWS Glue DataBrew im AWS Glue DataBrew -Entwicklerhandbuch.

Behebung von Risiken für Amazon-Notebook-Instances SageMaker

AWS Security Hub kann Risikopergebnisse für SageMaker Amazon-Notebook-Instances generieren.

Auf der Security Hub Hub-Konsole werden die Notebook-Instance, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einzelnes Problembehebungsergebnis umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

> **Note**
>
> Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- Merkmale von Fehlkonfigurationen für SageMaker Amazon-Notebook-Instances
  - Für die Amazon SageMaker Notebook-Instance ist direkter Internetzugang aktiviert
  - Für die SageMaker Amazon-Notebook-Instance ist der Root-Zugriff aktiviert
- Eigenschaften sensibler Daten für SageMaker Amazon-Notebook-Instances
  - Die SageMaker Amazon-Notebook-Instance enthält sensible Daten
- Auswirkungsmerkmale für Amazon SageMaker Notebook-Instances
  - Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

- Verfügt über einen direkten politischen Eskalationspfad
- Hat einen Hijack-Pfad für Vertrauensrichtlinien
- Hat einen Pfad zur Daten-Ransomware
- Hat den Beschränkungspfad entfernt
- Hat die Rolle bestanden, den Executor-Pfad erstellen
- Hat einen bestehenden Executor-Pfad für die Swap-Rolle
- Hat einen Eskalationspfad für die Rollenkette
- Hat einen privilegierten Executor-Pfad für Inject-Code
- Hat den Audit-Trail-Pfad deaktiviert
- Hat Zugriff auf den vorhandenen Executor-Pfad
- Hat einen Pfad zum Minting von Anmeldeinformationen
- Hat den Datenzugriffspfad bestanden
- Hat den Pfad zur Übernahme der Rolle, der Aufgabe zugewiesen
- Hat einen Single-Hop-Datenzugriffspfad
- Hat einen Pfad zur Weiterentwicklung der Fähigkeiten
- Geschäftliche Kritikalität

Merkmale von Fehlkonfigurationen für SageMaker Amazon-Notebook-Instances

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für SageMaker Amazon-Notebook-Instances und empfohlene Schritte zur Behebung.

Für die Amazon SageMaker Notebook-Instance ist direkter Internetzugang aktiviert

Wenn `DirectInternetAccess` es auf einer Amazon SageMaker Notebook-Instance aktiviert ist, wird ausgehender Datenverkehr über ein NAT-Gateway (SageMaker-managed Network Address Translation) ins Internet geleitet. Dies bietet einen Ausgangspfad, der für die Datenexfiltration oder als Befehls- und Kontrollkanal verwendet werden kann, falls das Notebook kompromittiert wurde. Deaktivieren Sie gemäß den bewährten Sicherheitsmethoden den direkten Internetzugang und platzieren Sie Notebook-Instances in einer VPC mit VPC-Endpunkten für die erforderlichen Dienste. AWS

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Deaktivieren des direkten Internetzugangs

Die `DirectInternetAccess` Einstellung kann nicht geändert werden, nachdem eine Notebook-Instanz erstellt wurde. Um es zu deaktivieren, erstellen Sie eine neue Notebook-Instanz mit der `DirectInternetAccess` Einstellung auf `Disabled` in einem privaten Subnetz innerhalb einer VPC und migrieren Sie dann Ihre Notebooks und Daten aus der vorhandenen Instanz. Anweisungen finden Sie im Amazon SageMaker Developer Guide unter Connect einer Notebook-Instance in einer VPC mit externen Ressourcen.

Konfigurieren von VPC-Endpunkten

Wenn der direkte Internetzugang deaktiviert ist, benötigt die Notebook-Instance VPC-Endpunkte, um auf AWS Dienste wie Amazon S3 und die SageMaker Amazon-API zuzugreifen. Erstellen Sie VPC-Endpoints mit Schnittstellen für die Dienste, die Ihr Notebook benötigt. Informationen zu VPC-Endpunkten finden Sie unter Was ist? AWS PrivateLink im Leitfaden.AWS PrivateLink

Für die SageMaker Amazon-Notebook-Instance ist der Root-Zugriff aktiviert

Wenn auf einer SageMaker Amazon-Notebook-Instance aktiviert `RootAccess` ist, haben Benutzer volle OS-level Root-Rechte. Der Root-Zugriff ermöglicht willkürliche Systemänderungen, persistente Backdoors und eine uneingeschränkte Paketinstallation. Halten Sie sich an bewährte Sicherheitsmethoden und deaktivieren Sie den Root-Zugriff für Notebook-Instanzen, sofern er nicht ausdrücklich für Ihren Workflow erforderlich ist.

Behebung: Deaktivieren Sie den Root-Zugriff

Sie können die `RootAccess` Einstellung auf einer laufenden Notebook-Instanz nicht ändern. Um sie zu deaktivieren, beenden Sie die Instanz und aktualisieren Sie dann die Instanzkonfiguration `RootAccess` auf`Disabled`. Die meisten Notebook-Workflows, einschließlich der Installation von Paketen mit `pip` und der Ausführung von Lebenszykluskonfigurationen, funktionieren auch ohne Root-Zugriff. Anweisungen finden Sie unter Steuern des Root-Zugriffs auf eine SageMaker Amazon-Notebook-Instance im Amazon SageMaker Developer Guide.

Weitere Überlegungen

Wenn für bestimmte Aufgaben Root-Zugriff erforderlich ist, sollten Sie stattdessen Amazon SageMaker Studio-Notebooks verwenden, die isolierte containerbasierte Umgebungen mit detaillierteren Zugriffskontrollen bieten. Sie können auch Lebenszykluskonfigurationen verwenden, um die erforderlichen Pakete bei der Erstellung der Instance vorzuinstallieren, sodass bei normalem Gebrauch weniger Root-Zugriff erforderlich ist.

Eigenschaften sensibler Daten für SageMaker Amazon-Notebook-Instances

Im Folgenden finden Sie die Merkmale sensibler Daten für Amazon SageMaker Notebook-Instances und empfohlene Schritte zur Problembehebung.

Die SageMaker Amazon-Notebook-Instance enthält sensible Daten

Ein Datensicherheitsscan hat bestätigt, dass sensible Daten auf der Amazon SageMaker Notebook-Instance vorhanden sind. Ein integriertes Datensicherheitsprodukt legt dieses Merkmal fest. Das Produkt überprüft die Dateien, Ausgaben und den angeschlossenen Speicher des Notebooks und identifiziert Inhalte, die geschützt werden müssen. Wir melden dieses Merkmal in Security Hub einheitlich, unabhängig davon, welches integrierte Produkt die Inspektion durchgeführt hat.

Sensible Daten erhöhen die Auswirkungen jeder anderen Schwachstelle auf derselben Notebook-Instanz. Durch eine permissive Ausführungsrolle, ein direkter Internetausgang oder ein zu breiter Zugriff werden regulierte oder vertrauliche Inhalte offengelegt. Ein Bedrohungsakteur, der das Notizbuch erreicht, kann diese Aufzeichnungen aus den Notebookdateien, Ausgabezellen und gespeicherten Checkpoints lesen und kopieren. Der Bedrohungsakteur kann diese Aufzeichnungen dann außerhalb Ihrer Umgebung aufbewahren. Sie können auch alle im Notizbuch enthaltenen Anmeldeinformationen verwenden, um sich bei anderen Systemen zu authentifizieren.

Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Zugriff auf Notebook-Instances zu beschränken, die vertrauliche Daten enthalten, und den angeschlossenen Speicher im Ruhezustand zu verschlüsseln.

Zu den sensiblen Daten können gehören:

- Anmeldeinformationen — wie Passwörter, Zugriffsschlüssel und Verbindungszeichenfolgen
- Persönlich identifizierbare Informationen
- Finanzinformationen — wie Kontonummern und Zahlungskartendaten
- Vertraulicher Inhalt, der geschützt werden muss

Das Entfernen der sensiblen Daten aus dem Notizbuch ist die einzige Möglichkeit, dieses Merkmal zu beseitigen. Wenn das Notizbuch auf vertrauliche Daten verweisen muss, verringern die folgenden bewährten Sicherheitsmethoden das Risiko einer Offenlegung.

Überprüfen Sie die vertraulichen Daten auf der Notebook-Instanz

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird die betroffene Notebook-Instanz geöffnet. Notieren Sie sich den Namen der Notebook-Instanz, das AWS Konto

und die AWS Region. Überprüfen Sie die Datensicherheitsfeststellung, die die vertraulichen Daten gemeldet hat, um festzustellen, welche Notebookdateien, Ausgabezellen oder Checkpoints sie enthalten.

Implementieren Sie je nach Art der entdeckten sensiblen Daten die entsprechenden Sicherheitskontrollen:

- Vertrauliche Werte aus dem Notizbuch entfernen — Löscht sensible Werte aus dem Notebookcode und löscht die Ausgabezellen, die sie enthalten. Löscht alle gespeicherten Prüfpunkte und exportierten Kopien, die die Werte beibehalten. Wenn ein Wert weiterhin referenziert werden muss, ersetzen Sie ihn durch einen Platzhalter in Tokens oder Maskierung. Weitere Informationen finden Sie unter Verwenden von Amazon SageMaker Notebook-Instances im Amazon SageMaker Developer Guide.
- Wechseln Sie alle offengelegten Anmeldeinformationen ab — Wenn das Notizbuch Anmeldeinformationen enthielt, behandeln Sie diese als gefährdet. Deaktivieren und rotieren Sie die Anmeldeinformationen und überprüfen Sie anschließend die Auditprotokolle des betroffenen Systems auf die Verwendung der offengelegten Werte. Rufen Sie geheime Daten zur Laufzeit aus AWS Secrets Manager einer eng begrenzten Ausführungsrolle ab, anstatt sie in den Notizbuchinhalt einzubetten. Weitere Informationen finden Sie im Benutzerhandbuch unter Rotation von AWS Secrets Manager Geheimnissen.AWS Secrets Manager
- Beschränken Sie, wer die Notebook-Instanz öffnen kann — Gewähren Sie nur den IAM-Identitäten Zugriff, die ihn benötigen. Ordnen Sie die Ausführungsrolle den spezifischen Aktionen und Ressourcen zu, die das Notebook verwendet. Steuern Sie, wer das Notizbuch öffnen kann, indem Sie die `sagemaker:CreatePresignedNotebookInstanceUrl` Zugriffsrechte einschränken. Weitere Informationen finden Sie in den Beispielen für SageMaker identitätsbasierte Richtlinien von Amazon im Amazon SageMaker Developer Guide.
- Den Notebook-Speicher im Ruhezustand verschlüsseln — Hängen Sie einen AWS KMS Schlüssel an die Notebook-Instance an, sodass das Speichervolume, auf dem sich die Notebook-Dateien und Checkpoints befinden, im Ruhezustand verschlüsselt wird. Verwenden Sie einen vom Kunden verwalteten Schlüssel, sodass Sie die Schlüsselrichtlinie kontrollieren können. `kms:Decrypt`Gewähren Sie diesen Schlüssel nur den Identitäten, die das Notizbuch lesen müssen. Weitere Informationen finden Sie unter Schützen von Daten im Ruhezustand mithilfe von Verschlüsselung im Amazon SageMaker Developer Guide.
- Überwachen Sie den Zugriff auf die Notebook-Instance — AWS CloudTrail Suchen Sie `sagemaker:CreatePresignedNotebookInstanceUrl` nach Anrufen und Zugriffen durch

unerwartete Identitäten oder Quellen. Weitere Informationen finden Sie unter SageMaker Amazon-API-Aufrufe protokollieren mit AWS CloudTrail im Amazon SageMaker Developer Guide.

Auswirkungsmerkmale für Amazon SageMaker Notebook-Instances

Die Wirkungsmerkmale beschreiben den potenziellen Explosionsradius einer Exposition. Security Hub analysiert die effektiven Berechtigungen des mit der SageMaker Notebook-Instanz verknüpften AWS Identity and Access Management Principals, um festzustellen, auf welche nachgelagerten Ressourcen ein Angreifer zugreifen könnte, wenn die Notebook-Instanz gefährdet ist, sowie die geschäftliche Bedeutung dieser Ressourcen. Jedes Auswirkungsmerkmal identifiziert ein bestimmtes Muster für die Eskalation von Rechten. Um deinen Explosionsradius zu verringern, überprüfe die in den einzelnen Merkmalen beschriebenen Berechtigungspfade und entferne alle unnötigen Rechte.

Gemäß den üblichen Sicherheitsprinzipien gewähren Sie geringste Rechte, indem Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Ersetzen Sie allgemeine Richtlinien durch spezifische Richtlinien, die nur die spezifischen Aktionen und Ressourcen gewähren, die benötigt werden. Verwenden Sie IAM Access Analyzer, um Empfehlungen auf der Grundlage des Zugriffsverlaufs zu generieren, um ungenutzte zu entfernende Berechtigungen zu identifizieren. Weitere Informationen finden Sie unter Ergebnisse für externen und ungenutzten Zugriff und Anwenden von Berechtigungen mit den geringsten Rechten im IAM-Benutzerhandbuch.

Verfügt über einen privilegierten Executor-Pfad mit Vollzugriff

Der zugehörige Principal kann einer Rechenressource, die bereits über erweiterte Berechtigungen verfügt, eine Rolle übergeben und Code in diese einschleusen. Auf diese Weise kann der Principal die volle Kontrolle über den Executor erlangen und alle Aktionen ausführen, die die Rolle des Executors zulässt.

Verfügt über einen direkten politischen Eskalationspfad

Der zugehörige Principal kann die IAM-Richtlinien direkt ändern, um sich selbst zusätzliche Berechtigungen zu gewähren und so seine eigenen Rechte ohne Zwischenressourcen zu erweitern.

Hat einen Hijack-Pfad für Vertrauensrichtlinien

Der zugehörige Principal kann die Vertrauensrichtlinie einer IAM-Rolle so ändern, dass er selbst diese Rolle übernehmen kann, wodurch er die Berechtigungen der Rolle erhält.

Hat einen Pfad zur Daten-Ransomware

Der zugehörige Principal kann Daten auf eine Weise verschlüsseln oder löschen, die für Ransomware verwendet werden könnte, z. B. durch Verschlüsseln von Amazon S3 S3-Objekten mit einem vom Kunden verwalteten AWS KMS Schlüssel und anschließendes Ändern der Schlüsselrichtlinie.

Hat den Beschränkungspfad entfernt

Der zugehörige Prinzipal kann Sicherheitseinschränkungen wie Zugriffsgrenzen, Dienststeuerungsrichtlinien oder ressourcenbasierte Policy-Deny-Statements aufheben und so die Möglichkeiten anderer Prinzipale oder der Ressource selbst erweitern.

Hat die Rolle bestanden, den Executor-Pfad erstellen

Der zugehörige Principal kann eine neue Rechenressource (z. B. eine Lambda-Funktion oder eine Amazon EC2 EC2-Instance) erstellen und ihr eine privilegierte Rolle zuweisen, wodurch seine eigenen Berechtigungen durch die neue Ressource effektiv gewaschen werden.

Hat einen bestehenden Executor-Pfad für die Swap-Rolle

Der zugehörige Principal kann die einer vorhandenen Rechenressource zugeordnete IAM-Rolle ändern und sie durch eine privilegiertere Rolle ersetzen, um den Zugriff zu eskalieren.

Hat einen Eskalationspfad für die Rollenkette

Der zugeordnete Principal kann eine Abfolge von Rollen übernehmen, wobei jede Rolle in der Kette über immer umfangreichere Berechtigungen verfügt, sodass letztendlich eine Rolle mit hohen Rechten erreicht wird.

Hat einen privilegierten Executor-Pfad für Inject-Code

Der zugehörige Principal kann Code in eine laufende Rechenressource mit erhöhten Rechten einfügen und dabei beliebige Operationen unter der privilegierten Rolle dieser Ressource ausführen.

Hat den Audit-Trail-Pfad deaktiviert

Der zugehörige Principal kann Protokollierungs- oder Überwachungsdienste deaktivieren CloudTrail, um beispielsweise während oder nach einer Eskalation effektiv seine Spuren zu verwischen.

Hat Zugriff auf den vorhandenen Executor-Pfad

Der zugehörige Principal kann eine bestehende Rechenressource aufrufen oder eine Verbindung zu einer vorhandenen Rechenressource herstellen und die ihr zugeordnete Rolle verwenden, um privilegierte Aktionen auszuführen.

Hat einen Pfad zum Minting von Anmeldeinformationen

Der zugehörige Prinzipal kann neue langfristige Anmeldeinformationen (wie Zugriffsschlüssel oder Anmeldeprofile) für andere Prinzipale erstellen und so persistente Zugriffspfade einrichten, die Passwortrotationen oder Sitzungsablaufzeiten überstehen.

Hat den Datenzugriffspfad bestanden

Der zugehörige Principal kann eine Dienstressource erstellen und ihr eine Rolle zuweisen, die Zugriff auf vertrauliche Daten hat, sodass er über die neue Ressource indirekt auf diese Daten zugreifen kann.

Hat den Pfad zur Übernahme der Rolle, der Aufgabe zugewiesen

Der zugehörige Principal kann eine Rolle an eine geplante oder ereignisgesteuerte Aufgabe übergeben (z. B. eine Lambda-Funktion, die durch ein Ereignis ausgelöst wird), sodass er beliebigen Code mit den Berechtigungen dieser Rolle ausführen kann.

Hat einen Single-Hop-Datenzugriffspfad

Der zugehörige Principal kann über seine vorhandenen Berechtigungen direkt auf vertrauliche Datenressourcen (wie Amazon S3 S3-Buckets oder DynamoDB-Tabellen) zugreifen, ohne dass zwischengeschaltete Eskalationsschritte erforderlich sind.

Hat einen Pfad zur Weiterentwicklung der Fähigkeiten

Der zugeordnete Principal verfügt über einen Pfad zur Eskalation von Rechten, der seine allgemeinen Fähigkeiten über das hinaus erweitert, was seine direkt zugewiesenen Berechtigungen vermuten lassen würden. Dies ist eine allgemeine Klassifizierung für Pfade, die keinem spezifischeren Muster entsprechen.

Geschäftliche Kritikalität

Die geschäftliche Wichtigkeit der Primärressource, die entweder durch Automatisierungsregeln oder durch Inferenz aus dem Namen und den Tags festgelegt wird.

Behebung von Risiken für virtuelle Azure-Maschinen

AWS Security Hub kann Risikoprüfungen für virtuelle Azure-Maschinen generieren.

Auf der Security Hub-Konsole werden die virtuelle Azure-Maschine, die an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Merkmale einer Fehlkonfiguration für virtuelle Azure-Maschinen
  - Die virtuelle Azure-Maschine verfügt über eine offene Netzwerksicherheitsgruppe
  - Die virtuelle Azure-Maschine verfügt über eine Sicherheitsregel, die den SSH- oder RDP-Zugriff ermöglicht
  - Der Rolle, die der virtuellen Azure-Maschine zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen
  - Die virtuelle Azure-Maschine hat ein Betriebssystem, das nicht mehr gültig ist
- Merkmale der Erreichbarkeit für virtuelle Azure-Maschinen
  - Die virtuelle Azure-Maschine ist über das Internet erreichbar
- Sicherheitsmerkmale für virtuelle Azure-Maschinen

- Die virtuelle Azure-Maschine weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist
- Die virtuelle Azure-Maschine weist Software-Sicherheitslücken auf
- Die virtuelle Azure-Maschine enthält schädliche Softwarepakete

Merkmale einer Fehlkonfiguration für virtuelle Azure-Maschinen

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für virtuelle Azure-Maschinen und empfohlene Korrekturmaßnahmen.

Die virtuelle Azure-Maschine verfügt über eine offene Netzwerksicherheitsgruppe

Eine Netzwerksicherheitsgruppe (NSG) fungiert als virtuelle Firewall für Ihre virtuelle Azure-Maschine und filtert eingehenden und ausgehenden Datenverkehr anhand einer Reihe von priorisierten Sicherheitsregeln. Eine offene Netzwerksicherheitsgruppe enthält Regeln, die den uneingeschränkten Zugriff von jeder Quelle aus ermöglichen (z. B. eine Quelle von oder). Any `0.0.0.0/0` Diese Regeln können Ihre virtuelle Maschine unberechtigtem Zugriff aus dem Internet aussetzen. Beschränken Sie die Regeln für Netzwerksicherheitsgruppen gemäß den Standardsicherheitsprinzipien auf die spezifischen IP-Adressen, Ports und Protokolle, die Ihre Arbeitslast benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Überprüfen Sie die Regeln für Netzwerksicherheitsgruppen und bewerten Sie die aktuelle Konfiguration

Identifizieren Sie die Netzwerksicherheitsgruppe, die der Netzwerkschnittstelle oder dem Subnetz der virtuellen Maschine zugeordnet ist, und überprüfen Sie die Sicherheitsregeln für eingehenden Datenverkehr. Prüfen Sie, welche Ports Datenverkehr aus breiten Quellbereichen zulassen, z. B. Any oder. `0.0.0.0/0` Regeln werden in der Reihenfolge ihrer Priorität verarbeitet. Stellen Sie daher sicher, dass eine zulässige Regel keinen Vorrang vor einer restriktiveren Regel hat. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerksicherheitsgruppen.

Schränken Sie die Regeln für Netzwerksicherheitsgruppen ein

Ändern oder entfernen Sie Regeln, die uneingeschränkten Zugriff ermöglichen. Ersetzen Sie eine breite Quelle, z. B. Any durch die spezifischen vertrauenswürdigen IP-Adressen, CIDR-Bereiche,

Service-Tags oder Anwendungssicherheitsgruppen, für die Zugriff erforderlich ist. Beschränken Sie den Zielportbereich auf die Ports, die Ihr Workload verwendet. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerksicherheitsgruppen verwalten.

Die virtuelle Azure-Maschine verfügt über eine Sicherheitsregel, die den SSH- oder RDP-Zugriff ermöglicht

Mit Fernverwaltungsprotokollen wie SSH (Port 22) und RDP (Port 3389) können Benutzer von Remote-Standorten aus eine Verbindung zu virtuellen Azure-Maschinen herstellen und diese verwalten. Wenn eine Netzwerksicherheitsgruppenregel diese Ports aus dem Internet zulässt (eine Quelle von `Any` oder`0.0.0.0/0`), vergrößert sich die Angriffsfläche Ihrer virtuellen Maschine erheblich und sie ist Brute-Force-Angriffen und Anmeldedaten ausgesetzt. Beschränken Sie den Fernzugriff gemäß den Standardsicherheitsprinzipien auf bestimmte, vertrauenswürdige IP-Adressen oder sperren Sie den direkten Internetzugriff auf diese Ports vollständig.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Schränken Sie die Gruppenregel für die Netzwerksicherheit ein

Beschränken Sie stattdessen den SSH- und RDP-Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder CIDR-BereicheAny, oder entfernen Sie die Regel für eingehenden Datenverkehr, wenn kein Fernzugriff aus dem Internet erforderlich ist. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerksicherheitsgruppen verwalten.

Verwenden Sie Azure Bastion für sichere Konnektivität

Anstatt SSH- oder RDP-Ports dem Internet zugänglich zu machen, verwenden Sie Azure Bastion, um über TLS eine Verbindung zu Ihrer virtuellen Maschine herzustellen, ohne eine öffentliche IP-Adresse zu haben oder eingehende Ports zu öffnen. Weitere Informationen finden Sie unter Azure Bastion in der Microsoft Azure-Dokumentation.

Verwenden Sie den Just-in-Time-Zugriff auf virtuelle Maschinen

Aktivieren Sie in Microsoft Defender for Cloud den Just-in-Time-Zugriff (JIT) auf virtuelle Maschinen, sodass Management-Ports wie SSH und RDP standardmäßig geschlossen bleiben und nur für genehmigte, zeitgebundene Anfragen von einer bestimmten Quell-IP-Adresse geöffnet sind. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Just-in-Time-Zugriff aktivieren.

Der Rolle, die der virtuellen Azure-Maschine zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen

Sie können einer virtuellen Azure-Maschine eine verwaltete Identität zuweisen und ihr Rollenzuweisungen für die rollenbasierte Zugriffskontrolle (Azure RBAC) für den Zugriff auf andere Azure-Ressourcen gewähren. Wenn der zugehörigen Identität eine administrative Rollenzuweisung (z. B. `Owner` oder`Contributor`) in einem breiten Umfang zugewiesen ist, gewährt sie in der Regel Berechtigungen, die weit über das hinausgehen, was für die Arbeitslast erforderlich ist. Wenn die virtuelle Maschine kompromittiert ist, kann ein Angreifer diese übermäßigen Berechtigungen nutzen, um sich quer durch Ihre Umgebung zu bewegen, auf Daten zuzugreifen oder Ressourcen zu manipulieren. Gewähren Sie gemäß den Standardsicherheitsprinzipien die geringsten Rechte, indem Sie nur die Berechtigungen zuweisen, die der Workload benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um diesem Risiko zu begegnen:

Überprüfen und identifizieren Sie die administrativen Rollenzuweisungen

Überprüfen Sie im Azure-Portal die Rollenzuweisungen für die Identität, die der virtuellen Maschine zugeordnet ist. Suchen Sie nach privilegierten Administratorrollen wie`Owner`, oder `Contributor`, `User Access Administrator`, und nach benutzerdefinierten Rollen, in deren `Actions` Rollen ein Platzhalterzeichen (`*`) verwendet wird. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure-Rollenzuweisungen auflisten.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie administrative Rollenzuweisungen durch die integrierte Rolle mit den geringsten Rechten, die nur die Berechtigungen gewährt, die für den Workload erforderlich sind. Weisen Sie sie im engsten Umfang (Ressource oder Ressourcengruppe) zu, der Ihren Anforderungen entspricht. Wenn Sie benutzerdefinierte Rollen erstellen, geben Sie `DataActions` explizit `Actions` und nicht einen Platzhalter ein. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Methoden für Azure RBAC.

Die virtuelle Azure-Maschine hat ein Betriebssystem, das nicht mehr gültig ist

Auf der virtuellen Azure-Maschine wird ein auslaufendes Betriebssystem ausgeführt, das vom Hersteller nicht mehr unterstützt oder gewartet wird. Wenn ein Betriebssystem das Ende seiner Lebensdauer erreicht, veröffentlicht der Anbieter keine Sicherheitsupdates und -hinweise mehr. Dadurch bleiben bekannte Sicherheitslücken dauerhaft ungepatcht und die virtuelle Maschine ist

Angriffen ausgesetzt. Führen Sie ein Upgrade auf eine unterstützte Betriebssystemversion gemäß den bewährten Sicherheitsmethoden durch.

Problembehebung: Führen Sie ein Upgrade auf eine unterstützte Betriebssystemversion durch

Planen Sie ein direktes Upgrade oder migrieren Sie die Arbeitslast auf eine virtuelle Maschine, auf der eine unterstützte Betriebssystemversion ausgeführt wird. Überprüfen Sie vor dem Upgrade die Anwendungskompatibilität und erstellen Sie ein Backup oder einen Snapshot, damit Sie bei Bedarf ein Rollback durchführen können. Folgen Sie für Windows den Upgrade-Anweisungen vor Ort; für Linux folgen Sie den Upgrade-Anweisungen Ihres Vertriebsanbieters. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Durchführen eines direkten Upgrades einer Windows Server-VM.

Merkmale der Erreichbarkeit für virtuelle Azure-Maschinen

Im Folgenden finden Sie Erreichbarkeitsmerkmale für virtuelle Azure-Maschinen und empfohlene Korrekturmaßnahmen.

Die virtuelle Azure-Maschine ist über das Internet erreichbar

Eine virtuelle Azure-Maschine mit Anschlüssen, die über das Internet erreichbar sind, ist möglicherweise einem Angriff ausgesetzt. Eine virtuelle Maschine wird erreichbar, wenn sie eine öffentliche IP-Adresse hat. Sie kann auch erreichbar werden, wenn ein Load Balancer, ein Anwendungsgateway oder ein anderer Netzwerkpfad eingehenden Datenverkehr aus dem Internet zulässt. Implementieren Sie Netzwerkzugriffskontrollen nach den üblichen Sicherheitsprinzipien, indem Sie den eingehenden Datenverkehr auf die erforderlichen Quellen und Ports beschränken.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Schränken Sie das Internetrisiko ein oder entfernen Sie es

Prüfen Sie, ob die virtuelle Maschine eine öffentliche IP-Adresse benötigt. Ist dies nicht der Fall, trennen Sie die öffentliche IP-Adresse von der Netzwerkschnittstelle und verwenden Sie stattdessen eine private IP-Adresse. Wenn weiterhin eine ausgehende Internetverbindung erforderlich ist, verwenden Sie ein NAT-Gateway.

Wenn eingehender Zugriff erforderlich ist, platzieren Sie die virtuelle Maschine hinter einem Load Balancer, einer Azure Firewall oder einem Anwendungsgateway, anstatt sie direkt zugänglich zu

machen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Öffentliche IP-Adressen.

Verschärfen Sie die Regeln für Sicherheitsgruppen für eingehende Netzwerke

Ändern oder entfernen Sie die Gruppenregeln für eingehende Netzwerke, die uneingeschränkten Zugriff ermöglichen (`Any`oder`0.0.0.0/0`), und beschränken Sie den Zugriff auf die spezifischen Quellbereiche, Ports und Protokolle, die Ihre Workload benötigt. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerksicherheitsgruppen.

Verwenden Sie Azure Bastion für den Verwaltungszugriff

Verwenden Sie für die Verwaltungskonnektivität Azure Bastion, um die virtuelle Maschine über TLS ohne öffentliche IP-Adresse oder offene SSH/RDP Ports zu erreichen. Weitere Informationen finden Sie unter Azure Bastion in der Microsoft Azure-Dokumentation.

Sicherheitsmerkmale für virtuelle Azure-Maschinen

Im Folgenden finden Sie Schwachstellenmerkmale für virtuelle Azure-Maschinen und empfohlene Maßnahmen zur Behebung.

Die virtuelle Azure-Maschine weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist

Common Vulnerabilities and Exposures (CVEs) können sich auf Softwarepakete auswirken, die auf virtuellen Azure-Maschinen installiert sind. Eine Sicherheitslücke mit hoher Priorität kann über das Netzwerk ausgenutzt werden, und es besteht eine hohe Wahrscheinlichkeit, dass sie ausgenutzt wird. Dies stellt eine unmittelbare Sicherheitsbedrohung dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Patchen Sie diese Sicherheitslücken umgehend, um Ihre virtuelle Maschine zu schützen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Überprüfen Sie den Befund und korrigieren Sie ihn

Verwenden Sie Microsoft Defender for Cloud Vulnerability Assessment, um die betroffenen CVEs und die Schritte zur Behebung der virtuellen Maschine zu überprüfen. Der Detailbereich für jedes Ergebnis enthält die relevanten CVEs und die empfohlenen Abhilfemaßnahmen.

Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Beheben von Computerschwachstellen.

Updates anwenden

Verwenden Sie Azure Update Manager, um Betriebssystem- und Softwareupdates auf Ihren virtuellen Maschinen nach einem Zeitplan zu bewerten und bereitzustellen. Wenn kein Update verfügbar ist, sollten Sie erwägen, die anfällige Software zu entfernen oder zu deaktivieren oder den Netzwerkzugriff darauf einzuschränken, bis ein Patch veröffentlicht wird. Weitere Informationen finden Sie unter Azure Update Manager in der Microsoft Azure-Dokumentation.

Zukünftige Überlegungen

Um zukünftige Ereignisse zu verhindern, aktivieren Sie Microsoft Defender for Servers so, dass Ihre virtuellen Maschinen kontinuierlich nach Sicherheitslücken durchsucht werden, und richten Sie mit Azure Update Manager einen regelmäßigen Patching-Zeitplan ein. Weitere Informationen finden Sie unter Microsoft Defender for Servers in der Microsoft Azure-Dokumentation.

Die virtuelle Azure-Maschine weist Software-Sicherheitslücken auf

Common Vulnerabilities and Exposures (CVEs) können sich auf Softwarepakete auswirken, die auf virtuellen Azure-Maschinen installiert sind. Bei unkritischen Sicherheitslücken handelt es sich um Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit als Sicherheitslücken mit hoher Priorität. Obwohl sie ein geringeres unmittelbares Risiko darstellen, können Angreifer ungepatchte Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Patchen Sie diese Sicherheitslücken gemäß den bewährten Sicherheitsmethoden, um Ihre virtuelle Maschine vor Angriffen zu schützen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Überprüfen Sie den Befund und korrigieren Sie ihn

Verwenden Sie Microsoft Defender for Cloud Vulnerability Assessment, um die betroffenen CVEs zu überprüfen und die Schritte zur Behebung im Bereich mit den Suchdetails zu befolgen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Beheben von Computerschwachstellen.

Updates anwenden

Verwenden Sie Azure Update Manager, um Betriebssystem- und Softwareupdates auf Ihren virtuellen Maschinen zu bewerten und bereitzustellen. Um Updates konsistent und in großem Umfang zu verwalten, konfigurieren Sie geplante Patches. Weitere Informationen finden Sie unter Azure Update Manager in der Microsoft Azure-Dokumentation.

Die virtuelle Azure-Maschine enthält schädliche Softwarepakete

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihre virtuelle Maschine dar, da Angreifer den Schadcode automatisch ausführen können, ohne eine separate Sicherheitslücke auszunutzen. Entfernen Sie bösartige Pakete gemäß den bewährten Sicherheitsmethoden, um Ihre virtuelle Maschine vor potenziellen Angriffen zu schützen.

Problembehebung: Untersuchen und entfernen Sie bösartige Pakete

Überprüfen Sie die Funddetails, um die Bedrohung zu verstehen und die betroffenen Pakete zu identifizieren. Entfernen Sie dann die identifizierten Pakete mithilfe des entsprechenden Paketmanagers für das Betriebssystem. Führen Sie nach dem Entfernen einen Scan durch, um sicherzustellen, dass keine verwandten schädlichen Komponenten mehr vorhanden sind. Weitere Informationen finden Sie unter Microsoft Defender for Servers in der Microsoft Azure-Dokumentation.

Behebung von Risiken für Azure Storage-Blob-Container

AWS Security Hub kann Risikoprüfungen für Azure Storage-Blob-Container generieren.

Auf der Security Hub-Konsole werden der Azure Storage-Blob-Container, der an einer Gefahrenfeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der Security Hub GetFindingsV2 CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Erreichbarkeitsmerkmale für Azure Storage-Blob-Container
  - Das Speicherkonto ermöglicht anonymen Blob-Zugriff
- Fehlkonfigurationsmerkmale für Azure Storage-Blob-Container
  - Das Speicherkonto benötigt kein HTTPS für Übertragungsvorgänge
  - Das Speicherkonto ist nicht mit vom Kunden verwalteten Schlüsseln verschlüsselt
  - Das Speicherkonto ermöglicht den mandantenübergreifenden Zugriff
  - Für das Speicherkonto ist Blob Soft Delete deaktiviert
  - Das Speicherkonto ermöglicht das dauerhafte Löschen von vorläufig gelöschten Blobs
  - Für den Azure Storage-Blob-Container ist die Blob-Versionierung deaktiviert
  - Für den Speichercontainer gibt es keine Unveränderlichkeitsrichtlinie

Erreichbarkeitsmerkmale für Azure Storage-Blob-Container

Im Folgenden finden Sie Erreichbarkeitsmerkmale für Azure Storage-Blob-Container und empfohlene Abhilfemaßnahmen.

Das Speicherkonto ermöglicht anonymen Blob-Zugriff

Wenn der anonyme Lesezugriff aktiviert ist, können nicht authentifizierte Clients Blob-Daten ohne Autorisierung lesen. Wenn das Speicherkonto anonymen (öffentlichen) Blob-Zugriff zulässt und die Zugriffsebene eines Containers dies zulässt, kann jeder im öffentlichen Internet die Daten in diesem Container lesen. Verbieten Sie gemäß den Standardsicherheitsprinzipien den anonymen Zugriff auf Kontoebene und verlangen Sie, dass jede Anfrage autorisiert wird, es sei denn, Ihr Szenario hängt ausdrücklich vom öffentlichen Lesezugriff ab.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Verbieten Sie den anonymen Zugriff auf das Speicherkonto

Stellen Sie die `AllowBlobPublicAccess` Eigenschaft des Speicherkontos auf ein`false`. Wenn Sie den anonymen Zugriff auf Kontoebene verbieten, werden die Zugriffseinstellungen aller Container im Konto außer Kraft gesetzt und zukünftige anonyme Anfragen blockiert. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Anonymen Lesezugriff verhindern.

Stellen Sie die Container-Zugriffsebene auf privat ein

Wenn einzelne Container für den öffentlichen Zugriff konfiguriert wurden, setzen Sie die anonyme Zugriffsebene jedes Containers auf, `Private` sodass für alle Anfragen eine Autorisierung erforderlich ist. Bevor Sie die Einstellung ändern, überprüfen Sie alle Client-Anwendungen, die möglicherweise auf anonymen Zugriff angewiesen sind. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Konfigurieren des anonymen Lesezugriffs.

Fehlkonfigurationsmerkmale für Azure Storage-Blob-Container

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Storage-Blob-Container und empfohlene Behebungsschritte.

Das Speicherkonto benötigt kein HTTPS für Übertragungsvorgänge

Wenn ein Speicherkonto keine sichere Übertragung erfordert, akzeptiert es Anfragen über unverschlüsseltes HTTP. Über HTTP gesendete Daten und Anmeldeinformationen können während der Übertragung von einem Angreifer auf dem Netzwerkpfad abgefangen oder geändert werden. Erfordern Sie gemäß den Standardsicherheitsprinzipien eine sichere Übertragung, sodass das Konto Anfragen nur über HTTPS akzeptiert.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Sichere Übertragung erforderlich

Aktivieren Sie die Eigenschaft Sichere Übertragung erforderlich auf dem Speicherkonto (das `enableHttpsTrafficOnly` Objekt). Wenn eine sichere Übertragung erforderlich ist, wird jede

über HTTP gestellte Anfrage abgelehnt. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Sichere Übertragung erforderlich.

Erzwingen Sie eine Mindestversion von TLS

Stellen Sie die TLS-Mindestversion des Speicherkontos auf 1.2 (die `minimumTlsVersion` Eigenschaft) ein, sodass Anfragen, die ältere, weniger sichere Protokollversionen verwenden, abgelehnt werden. Vergewissern Sie sich, dass Ihre Clients TLS 1.2 unterstützen, bevor Sie diese Einstellung erzwingen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Konfigurieren der TLS-Mindestversion für ein Speicherkonto.

Das Speicherkonto ist nicht mit vom Kunden verwalteten Schlüsseln verschlüsselt

Standardmäßig verschlüsselt Azure Storage gespeicherte Daten mit Microsoft-managed Schlüsseln. Customer-managed Mit Schlüsseln (CMK) haben Sie die Kontrolle über den Schlüssel, der Ihre Daten schützt. Dazu gehört auch die Möglichkeit, den Zugriff auf den Schlüssel zu rotieren, zu widerrufen und zu überprüfen. Wenn die Compliance-Anforderungen Ihres Unternehmens die Kontrolle über Verschlüsselungsschlüssel erfordern, ist das Fehlen von vom Kunden verwalteten Schlüsseln eine Lücke. Konfigurieren Sie das Speicherkonto gemäß den bewährten Methoden für den Datenschutz so, dass vom Kunden verwaltete Schlüssel verwendet werden, die in Azure Key Vault oder einem verwalteten HSM gespeichert sind.

Problembehebung: Konfigurieren Sie vom Kunden verwaltete Schlüssel

Speichern Sie einen Schlüssel in Azure Key Vault oder Azure Key Vault Managed HSM, wobei der Schutz vor automatischem Löschen und Löschen aktiviert ist. Gewähren Sie einer verwalteten Identität die `unwrapkey` Berechtigungen `getwrapkey`,, und konfigurieren Sie dann das Speicherkonto so, dass dieser Schlüssel für die Verschlüsselung verwendet wird. Sie können jederzeit zwischen vom Kunden verwalteten Microsoft-managed Schlüsseln und Schlüsseln wechseln. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Customer-managed Schlüssel für die Speicherverschlüsselung.

Das Speicherkonto ermöglicht den mandantenübergreifenden Zugriff

Cross-tenant Zugriffseinstellungen, wie z. B. mandantenübergreifende Objektreplikation oder mandantenübergreifende SAS-Delegierung (Shared Access Signature), können dazu führen, dass Daten den Microsoft Entra-Mandanten verlassen, dem das Speicherkonto gehört. Wenn für Ihre Arbeitslast keine gemeinsame Nutzung von Daten zwischen Mandanten erforderlich ist, erhöht sich das Risiko, dass Daten Ihre Mandantengrenze verlassen, wenn Sie diese

Einstellungen aktiviert lassen. Deaktivieren Sie den mandantenübergreifenden Zugriff gemäß den Standardsicherheitsprinzipien, sofern er nicht ausdrücklich erforderlich ist.

Problembehebung: Deaktivieren Sie die Einstellungen für den mandantenübergreifenden Zugriff

Deaktivieren Sie auf dem Speicherkonto die mandantenübergreifende Objektreplikation (auf gesetzt `allowCrossTenantReplicationfalse`) und schränken Sie, sofern unterstützt, die mandantenübergreifende SAS-Delegierung ein. Überprüfen Sie Ihre Anforderungen für Replikation und gemeinsame Nutzung, bevor Sie die Änderung vornehmen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Übersicht über das Azure Storage-Konto.

Für das Speicherkonto ist Blob Soft Delete deaktiviert

Blob Soft Delete schützt einzelne Blobs, Snapshots und Versionen vor versehentlichem oder böswilligem Löschen und Überschreiben. Die gelöschten Daten werden für einen konfigurierbaren Aufbewahrungszeitraum aufbewahrt, in dem Sie sie wiederherstellen können. Wenn das automatische Löschen deaktiviert ist, können gelöschte oder überschriebene Blob-Daten nicht wiederhergestellt werden, wodurch Ihr Konto einem dauerhaften Datenverlust ausgesetzt ist. Aktivieren Sie das automatische Löschen von Blobs mit einer angemessenen Aufbewahrungsfrist gemäß den bewährten Datenschutzpraktiken.

Problembehebung: Aktivieren Sie das automatische Löschen von Blobs

Aktivieren Sie das automatische Löschen von Blobs für das Speicherkonto und legen Sie einen Aufbewahrungszeitraum (1 bis 365 Tage) fest, der Ihren Wiederherstellungsanforderungen entspricht. Für einen umfassenderen Schutz aktivieren Sie auch das Soft-Delete von Containern und die Blob-Versionierung. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Soft-Delete für Blobs.

Das Speicherkonto ermöglicht das dauerhafte Löschen von vorläufig gelöschten Blobs

Wenn permanentes Löschen zulässig ist (die `allowPermanentDelete` Eigenschaft lautet`true`), können vorläufig gelöschte Blobs und Snapshots entfernt werden, bevor die Aufbewahrungsfrist für das vorläufige Löschen abläuft. Dies untergräbt den Schutz, den Soft-Delete bietet, da ein Benutzer oder ein kompromittierter Principal wiederherstellbare Daten vor Ablauf der Aufbewahrungsfrist dauerhaft vernichten kann. Erlauben Sie gemäß den bewährten Datenschutzpraktiken kein dauerhaftes Löschen von temporär gelöschten Blobs, es sei denn, Sie haben eine bestimmte, wohlverstandene Anforderung.

Behebung: Deaktivieren Sie das dauerhafte Löschen

Stellen Sie die `allowPermanentDelete` Eigenschaft des Speicherkontos auf `false` so ein, dass vorläufig gelöschte Blobs und Snapshots während des gesamten Aufbewahrungszeitraums wiederhergestellt werden können. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Soft-Delete für Blobs.

Für den Azure Storage-Blob-Container ist die Blob-Versionierung deaktiviert

Bei der Blob-Versionierung werden frühere Versionen eines Blobs automatisch beibehalten. Wenn ein Blob geändert oder gelöscht wird, wird der vorherige Status als frühere Version beibehalten, die Sie wiederherstellen können. Wenn die Versionsverwaltung deaktiviert ist, können Überschreibungen und Löschungen nicht auf einen früheren Status zurückgesetzt werden, wodurch das Risiko eines nicht wiederherstellbaren Datenverlusts oder einer Datenbeschädigung steigt. Halten Sie sich an die bewährten Datenschutzmethoden und aktivieren Sie die Blob-Versionierung zusammen mit Soft-Delete, um einen optimalen Datenschutz zu gewährleisten.

Problembehebung: Aktivieren Sie die Blob-Versionierung

Aktivieren Sie die Versionierung im BLOB-Dienst des Speicherkontos. Um die Kosten für die Aufbewahrung vieler Versionen zu kontrollieren, verwenden Sie eine Lifecycle-Management-Richtlinie, um alte Versionen automatisch zu löschen. Weitere Informationen finden Sie unter Blob-Versionierung in der Microsoft Azure-Dokumentation.

Für den Speichercontainer gibt es keine Unveränderlichkeitsrichtlinie

Eine Unveränderlichkeitsrichtlinie speichert Blob-Daten im WORM-Zustand (Write Once, Read Many). In diesem Zustand können Daten für ein bestimmtes Intervall (eine zeitbasierte Aufbewahrungsrichtlinie) oder bis eine gesetzliche Aufbewahrungsfrist aufgehoben ist, nicht geändert oder gelöscht werden. Ohne eine Unveränderbarkeitsrichtlinie können geschäftskritische oder Compliance-relevante Daten im Container überschrieben oder gelöscht werden, auch von berechtigten Benutzern. Wenn gesetzliche Vorschriften oder Datenintegritätsanforderungen gelten, konfigurieren Sie eine Unveränderbarkeitsrichtlinie für den Container.

Behebung: Konfigurieren Sie eine Unveränderlichkeitsrichtlinie

Konfigurieren Sie eine zeitbasierte Aufbewahrungsrichtlinie oder eine gesetzliche Aufbewahrungsfrist für den Container. Sperren Sie die zeitbasierte Richtlinie, wenn die Tests abgeschlossen sind, sodass die Daten im WORM-Status vollständig geschützt sind. Aktivieren Sie das automatische Löschen, bevor Sie Richtlinien zur Unveränderlichkeit anwenden, um zusätzlichen Schutz zu gewährleisten. Weitere Informationen finden Sie unter Unveränderlicher Speicher für Blob-Daten in der Microsoft Azure-Dokumentation.

Behebung von Risiken für Azure SQL-Datenbanken

AWS Security Hub kann Risikenergebnisse für Azure SQL-Datenbanken generieren.

Auf der Security Hub-Konsole werden die Azure SQL-Datenbank, die an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure SQL-Datenbanken
  - Für die Azure SQL-Datenbank ist der öffentliche Netzwerkzugriff aktiviert
  - Die Azure SQL-Datenbank erzwingt keine AD-only Azure-Authentifizierung
  - Die Azure SQL-Datenbank verwendet einen standardmäßigen oder allgemeinen Admin-Benutzernamen
  - Für die Azure SQL-Datenbank ist die georedundante Sicherung deaktiviert

Fehlkonfigurationsmerkmale für Azure SQL-Datenbanken

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure SQL-Datenbanken und empfohlene Korrekturmaßnahmen.

Für die Azure SQL-Datenbank ist der öffentliche Netzwerkzugriff aktiviert

Wenn der öffentliche Netzwerkzugriff auf dem logischen Server aktiviert ist, ist die Datenbank über einen öffentlichen Endpunkt erreichbar und kann Verbindungen aus dem öffentlichen Internet akzeptieren (vorbehaltlich der Firewallregeln). Ein öffentlicher Endpunkt vergrößert die Angriffsfläche Ihrer Datenbank und setzt sie unbefugten Verbindungsversuchen aus. Deaktivieren Sie gemäß den Standardsicherheitsprinzipien den öffentlichen Netzwerkzugriff und stellen Sie eine private Verbindung zur Datenbank her, oder schränken Sie die Serverfirewallregeln strikt ein.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Deaktivieren Sie den öffentlichen Netzwerkzugriff und verwenden Sie Private Link

Stellen Sie den öffentlichen Netzwerkzugriff des logischen Servers auf einen privaten Endpunkt (Azure Private Link) in Ihrem virtuellen Netzwerk ein `Disabled` und stellen Sie über einen privaten Endpunkt (Azure Private Link) eine Verbindung zur Datenbank her. Dadurch wird der Datenbankverkehr auf dem Azure-Backbone und vom öffentlichen Internet ferngehalten. Weitere Informationen finden Sie unter Netzwerkzugriffskontrollen für Azure SQL-Datenbanken in der Microsoft Azure-Dokumentation.

Schränken Sie die Firewallregeln ein, wenn öffentlicher Zugriff erforderlich ist

Wenn Sie den öffentlichen Zugriff aktiviert lassen müssen, entfernen Sie alle Regeln, die die gesamte Internetreichweite zulassen, und deaktivieren Sie die Option Azure-Diensten und -Ressourcen den Zugriff auf diesen Server gestatten, wenn sie nicht benötigt werden. Beschränken Sie die Firewallregeln auf Serverebene auf die spezifischen vertrauenswürdigen IP-Adressen, die Ihr Workload benötigt. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerkzugriffskontrollen für Azure SQL-Datenbanken.

Erzwingen Sie eine Mindestversion von TLS

Stellen Sie die TLS-Mindestversion des logischen Servers auf 1.2 ein, sodass Verbindungen, die ältere, weniger sichere Protokollversionen verwenden, abgelehnt werden. Vergewissern Sie sich, dass Ihre Clients TLS 1.2 unterstützen, bevor Sie diese Einstellung erzwingen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Konnektivitätseinstellungen für die Azure SQL-Datenbank.

Die Azure SQL-Datenbank erzwingt keine AD-only Azure-Authentifizierung

Wenn die Entra-only Microsoft-Authentifizierung (früher AD-only Azure-Authentifizierung) nicht erzwungen wird, akzeptiert der logische Server auch die SQL-Authentifizierung, die auf Kennwörtern basiert, die in der Datenbank gespeichert und verwaltet werden. Die SQL-Authentifizierung ist anfälliger für den Diebstahl von Anmeldeinformationen und Brute-Force-Angriffen und profitiert nicht von zentralisierten Microsoft Entra-Kontrollen wie bedingtem Zugriff und Multifaktor-Authentifizierung. Erzwingen Sie gemäß den Standardsicherheitsprinzipien die Entra-only Microsoft-Authentifizierung, sodass nur Microsoft Entra-Identitäten eine Verbindung herstellen können.

Abhilfe: Erzwingen Sie die Microsoft-Authentifizierung Entra-only

Richten Sie einen Microsoft Entra-Administrator für den logischen Server ein und aktivieren Sie dann die Entra-only Microsoft-Authentifizierung. Dadurch wird die SQL-Authentifizierung deaktiviert, sodass nur Microsoft Entra-Identitäten eine Verbindung zum Server und seinen Datenbanken herstellen können. Vergewissern Sie sich, dass Ihre Anwendungen die Microsoft Entra-Authentifizierung unterstützen, bevor Sie diese Einstellung durchsetzen. Weitere Informationen finden Sie unter Entra-only Microsoft-Authentifizierung in der Microsoft Azure-Dokumentation.

Die Azure SQL-Datenbank verwendet einen standardmäßigen oder allgemeinen Admin-Benutzernamen

Die Administratoranmeldung des logischen Servers verwendet einen bekannten oder gebräuchlichen Benutzernamen, z. B. `sqladminadmin`, oder`sa`. Gängige Administrator-Benutzernamen sind vorhersehbar, was den Server zu einem leichteren Ziel für Brute-Force- und Credential-Stuffing-Angriffe macht, da ein Angreifer nur das Passwort erraten muss. Vermeiden Sie standardmäßige oder allgemeine Administratorbenutzernamen gemäß den üblichen Sicherheitsprinzipien und zentralisieren Sie den Administratorzugriff über die Microsoft Entra ID.

Abhilfe: Verwenden Sie einen nicht standardmäßigen Administrator und die Microsoft Entra-Authentifizierung

Vermeiden Sie vorhersehbare Administrator-Anmeldenamen. Wenn möglich, sollten Sie die Entra-only Microsoft-Authentifizierung erzwingen und den Administratorzugriff über Microsoft Entra-Identitäten und -Gruppen statt über eine SQL-Administratoranmeldung verwalten. Folgen Sie den bewährten Azure SQL-Sicherheitsmethoden für die Verwaltung von Anmeldungen und Zugriffen mit geringsten Rechten. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Sicherheitsmethoden für Azure SQL-Datenbanken.

Für die Azure SQL-Datenbank ist die georedundante Sicherung deaktiviert

Die Azure SQL-Datenbank speichert automatische Backups standardmäßig in einem georedundanten Speicher, der Backups in eine gepaarte Region repliziert und die Geowiederherstellung bei einem regionalen Ausfall ermöglicht. Wenn die Backup-Speicherredundanz stattdessen auf lokal redundanten oder zonenredundanten Speicher eingestellt ist, ist die Geowiederherstellung nicht verfügbar. Sie können die Datenbank in einer anderen Region nicht wiederherstellen, wenn die primäre Region nicht mehr verfügbar ist. Verwenden Sie gemäß den bewährten Methoden zum Datenschutz georedundanten Backup-Speicher für Datenbanken, die gegen regionale Ausfälle gewappnet sein müssen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um diesem Risiko zu begegnen:

Konfigurieren Sie den georedundanten Backup-Speicher

Stellen Sie die Backup-Speicherredundanz der Datenbank auf georedundanten Speicher (GRS) oder geozonenredundanten Speicher (GZRS) ein, damit die Geowiederherstellung verfügbar ist. Änderungen gelten für zukünftige Backups und es kann bis zu 48 Stunden dauern, bis sie wirksam werden. Weitere Informationen finden Sie unter Automatisierte Backups in der Azure SQL-Datenbank in der Microsoft Azure-Dokumentation.

Konfigurieren Sie die langfristige Aufbewahrung

Für Datenbanken mit Konformitäts- oder Langzeitwiederherstellungsanforderungen konfigurieren Sie eine Richtlinie zur langfristigen Aufbewahrung (LTR). LTR bewahrt vollständige Backups zusätzlich zur standardmäßigen kurzfristigen Aufbewahrung bis zu 10 Jahre lang auf. Weitere Informationen finden Sie unter Long-term Aufbewahrung in der Azure SQL-Datenbank in der Microsoft Azure-Dokumentation.

Korrigieren von Risiken für Azure Cosmos DB-Konten

AWS Security Hub kann Risikoprüfungen für Azure Cosmos DB-Konten generieren.

Auf der Security Hub-Konsole werden das Azure Cosmos DB-Konto, das an einer Gefahrenfeststellung beteiligt war, und die zugehörigen Identifikationsinformationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der Security Hub GetFindingsV2 CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure Cosmos DB-Konten
  - Für das Azure Cosmos DB-Konto ist der öffentliche Netzwerkzugriff aktiviert
  - Das Azure Cosmos DB-Konto verwendet keine kontinuierliche Sicherung

Fehlkonfigurationsmerkmale für Azure Cosmos DB-Konten

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Cosmos DB-Konten und empfohlene Abhilfemaßnahmen.

Für das Azure Cosmos DB-Konto ist der öffentliche Netzwerkzugriff aktiviert

Wenn der öffentliche Netzwerkzugriff aktiviert ist, ist das Azure Cosmos DB-Konto über einen öffentlichen Endpunkt erreichbar. Es kann Verbindungen aus dem öffentlichen Internet akzeptieren, sofern die Firewall und die Regeln für virtuelle Netzwerke eingehalten werden. Ein öffentlicher Endpunkt vergrößert die Angriffsfläche Ihres Kontos und setzt es unbefugten Verbindungsversuchen und potenziellem Datendiebstahl aus. Deaktivieren Sie gemäß den Standardsicherheitsprinzipien den öffentlichen Netzwerkzugriff und stellen Sie eine private Verbindung zum Konto her oder schränken Sie die Firewallregeln des Kontos stark ein.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Deaktivieren Sie den öffentlichen Netzwerkzugriff und verwenden Sie Private Link

Stellen Sie die `publicNetworkAccess` Eigenschaft des Kontos auf einen privaten Endpunkt (Azure Private Link) in Ihrem virtuellen Netzwerk ein `Disabled` und stellen Sie eine Verbindung über einen privaten Endpunkt (Azure Private Link) her. In Kombination mit restriktiven Gruppenrichtlinien für Netzwerksicherheit tragen private Endpunkte dazu bei, das Risiko einer Datenexfiltration zu verringern. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure Private Link konfigurieren.

Schränken Sie die Firewallregeln ein, wenn öffentlicher Zugriff erforderlich ist

Wenn Sie den öffentlichen Zugriff aktiviert lassen müssen, konfigurieren Sie IP-Firewallregeln und virtuelle Netzwerkregeln so, dass nur die spezifischen vertrauenswürdigen Quellen zugelassen werden, die Ihre Arbeitslast benötigt, und nicht alle Netzwerke. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Konfigurieren der IP-Firewall.

Das Azure Cosmos DB-Konto verwendet keine kontinuierliche Sicherung

Im Modus „Kontinuierliche Sicherung“ können Sie die Point-in-Time-Wiederherstellung verwenden, um nach einem versehentlichen Schreib- oder Löschvorgang eine Wiederherstellung durchzuführen. Sie können auch eine gelöschte Datenbank oder einen gelöschten Container mit einem beliebigen Zeitstempel innerhalb des Aufbewahrungszeitraums wiederherstellen. Wenn das Konto den Modus für regelmäßige Backups anstelle der kontinuierlichen Sicherung verwendet, können Sie keine Self-Service-Point-in-Time-Wiederherstellung durchführen. Diese Einschränkung erhöht die Wiederherstellungszeit und erhöht das Risiko eines Datenverlusts nach einer versehentlichen oder böswilligen Änderung. Aktivieren Sie den kontinuierlichen Backup-Modus gemäß den Best Practices für den Datenschutz, sofern Ihr Workload dies unterstützt.

Problembehebung: Aktivieren Sie den kontinuierlichen Backup-Modus

Konfigurieren Sie das Konto für den kontinuierlichen Backup-Modus (7-Tage- oder 30-Tage-Tarif), sodass eine Wiederherstellung zu einem bestimmten Zeitpunkt möglich ist. Informieren Sie sich über die aktuellen Einschränkungen und unterstützten APIs, bevor Sie von einem regelmäßigen auf ein kontinuierliches Backup umsteigen. Weitere Informationen finden Sie unter Kontinuierliches Backup mit Point-in-Time-Wiederherstellung in der Microsoft Azure-Dokumentation.

Behebung von Risiken für Azure Function-Apps

AWS Security Hub kann Risikoprüfungen für Azure Function-Apps generieren.

Auf der Security Hub-Konsole werden die Azure Function-App, die an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure Function-Apps
  - Die Azure Function-App wird außerhalb eines VNet bereitgestellt
  - Der Rolle, die der Azure Function-App zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen
- Merkmale der Erreichbarkeit für Azure Function-Apps
  - Die Azure Function-App ermöglicht den anonymen Aufruf von HTTP-Triggern
- Sicherheitsmerkmale für Azure Function-Apps
  - Die Azure Function-App weist über das Netzwerk ausnutzbare Softwareschwachstellen auf, deren Ausnutzungswahrscheinlichkeit hoch ist
  - Die Azure Function-App weist Software-Sicherheitslücken auf
  - Die Azure Function-App enthält schädliche Softwarepakete

Fehlkonfigurationsmerkmale für Azure Function-Apps

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Function-Apps und empfohlene Korrekturmaßnahmen.

Die Azure Function-App wird außerhalb eines VNet bereitgestellt

Wenn eine Function-App nicht in ein virtuelles Netzwerk integriert ist, passieren ihre Endpunkte und der ausgehende Datenverkehr das öffentliche Netzwerk und nicht Ihre private Netzwerkgrenze. Wenn die Funktions-App nicht in ein virtuelles Netzwerk integriert ist, können Sie keine Kontrollen auf Netzwerkebene wie private Endpunkte, Netzwerksicherheitsgruppen und eingeschränkten ausgehenden Zugriff anwenden. Diese Lücke erhöht das Risiko der App. Integrieren Sie die Function-App gemäß den Standardsicherheitsprinzipien in ein virtuelles Netzwerk und verwenden Sie private Endpunkte, sofern Ihr Hosting-Paket dies unterstützt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um diesem Risiko zu begegnen:

Integrieren Sie die Function-App in ein virtuelles Netzwerk

Aktivieren Sie die virtuelle Netzwerkintegration für die Function-App. Verwenden Sie private Endpunkte, sodass die App nur von Ihrem Netzwerk aus erreichbar ist, sofern dies von Ihrem Hosting-Tarif (Flex Consumption, Elastic Premium oder Dedicated) unterstützt wird. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Netzwerkoptionen für Azure Functions.

Beschränken Sie den eingehenden Zugriff

Verwenden Sie bei Hostingplänen, die keine privaten Endpunkte unterstützen, Zugriffsbeschränkungen, um eingehenden Datenverkehr nur aus vertrauenswürdigen IP-Adressbereichen zuzulassen, und deaktivieren Sie den öffentlichen Netzwerkzugriff, wenn er nicht erforderlich ist. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Einrichten von Zugriffsbeschränkungen.

Der Rolle, die der Azure Function-App zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen

Sie können einer Azure Function-App eine verwaltete Identität zuweisen und ihr die rollenbasierte Azure-Zugriffskontrolle (Azure RBAC) -Rollenzuweisungen für den Zugriff auf andere Azure-Ressourcen gewähren. Wenn der zugehörigen Identität eine administrative Rollenzuweisung (z. B. `Owner` oder`Contributor`) in einem breiten Umfang zugewiesen ist, gewährt sie in der Regel

Berechtigungen, die weit über das hinausgehen, was die App benötigt. Wenn die Function-App kompromittiert ist, kann ein Angreifer diese übermäßigen Berechtigungen nutzen, um sich quer durch Ihre Umgebung zu bewegen, auf Daten zuzugreifen oder Ressourcen zu manipulieren. Gewähren Sie gemäß den Standardsicherheitsprinzipien die geringsten Rechte, indem Sie nur die Berechtigungen zuweisen, die die App benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um diesem Risiko zu begegnen:

Überprüfen und identifizieren Sie die administrativen Rollenzuweisungen

Überprüfen Sie im Azure-Portal die Rollenzuweisungen auf die Identität, die der Function-App zugeordnet ist. Suchen Sie nach privilegierten Administratorrollen wie`Owner`, oder `ContributorUser Access Administrator`, und nach benutzerdefinierten Rollen, in deren `Actions` Rollen ein Platzhalterzeichen (`*`) verwendet wird. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure-Rollenzuweisungen auflisten.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie administrative Rollenzuweisungen durch die integrierte Rolle mit den geringsten Rechten, die nur die Berechtigungen gewährt, die die App benötigt, und weisen Sie sie im engsten Umfang zu, der Ihren Anforderungen entspricht. Verwenden Sie eine verwaltete Identität anstelle von gespeicherten Geheimnissen für Verbindungen zu anderen Azure-Diensten. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Methoden für Azure RBAC.

Merkmale der Erreichbarkeit für Azure Function-Apps

Im Folgenden finden Sie Erreichbarkeitsmerkmale für Azure Function-Apps und empfohlene Abhilfemaßnahmen.

Die Azure Function-App ermöglicht den anonymen Aufruf von HTTP-Triggern

Eine HTTP-triggered Funktion, deren Autorisierungsstufe auf eingestellt ist, `anonymous` kann ohne Zugriffsschlüssel oder Authentifizierung über das Internet aufgerufen werden. Anonyme HTTP-Trigger machen Ihre Funktionslogik für nicht authentifizierte Aufrufer zugänglich, was zu Missbrauch, Datenpreisgabe oder einem Denial-of-Wallet durch unkontrollierten Aufruf führen kann. Erfordern Sie gemäß den Standardsicherheitsprinzipien Authentifizierungs- oder Zugriffsschlüssel für Funktionen, es sei denn, ein anonymer Zugriff ist ausdrücklich erforderlich. HTTP-triggered

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Autorisierung für HTTP-Trigger erforderlich

Erhöhen Sie die Autorisierungsstufe für HTTP-Trigger von `anonymous` auf `function` oder `admin` so, dass Anfragen einen gültigen Zugriffsschlüssel enthalten müssen und HTTPS erfordern. Für einen stärkeren Schutz aktivieren Sie App Service Authentication/Authorization oder verwenden Sie Azure API Management als Frontend für die App. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Securing Azure Functions.

Erfordern Sie eine Authentifizierung bei einem verwalteten Identitätsanbieter

Da Zugriffsschlüssel eher eine Autorisierungskontrolle als eine Authentifizierung sind, sollten Sie die App Service-Authentifizierung (Easy Auth) mit der Microsoft Entra-ID aktivieren, sodass Anrufer eine gültige Identität vorlegen müssen. Deaktivieren Sie auch die administrativen Endpunkte (die `/admin` Routen), wenn sie nicht benötigt werden. Weitere Informationen finden Sie unter Securing Azure Functions in der Microsoft Azure-Dokumentation.

Sicherheitsmerkmale für Azure Function-Apps

Im Folgenden finden Sie Schwachstellenmerkmale für Azure Function-Apps und empfohlene Maßnahmen zur Behebung.

Die Azure Function-App weist über das Netzwerk ausnutzbare Softwareschwachstellen auf, deren Ausnutzungswahrscheinlichkeit hoch ist

Common Vulnerabilities and Exposures (CVEs) können sich auf Softwarepakete und Abhängigkeiten in Ihrer Function-App auswirken. Eine Sicherheitslücke mit hoher Priorität ist vom Netzwerk ausnutzbar und bietet eine hohe Wahrscheinlichkeit, dass sie ausgenutzt wird. Dies stellt eine unmittelbare Sicherheitsbedrohung dar, da der Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern aktiv genutzt wird. Patchen Sie diese Sicherheitslücken umgehend, um Ihre Function-App zu schützen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Aktualisieren Sie die betroffenen Abhängigkeiten

Überprüfen Sie die betroffenen CVEs im Ergebnis, aktualisieren Sie dann die anfälligen Pakete und Abhängigkeiten auf die neuesten sicheren Versionen und stellen Sie die App erneut bereit. Verwenden Sie die Function-App auf einer unterstützten Laufzeit, damit die Sicherheitsupdates für

die Plattform weiterhin gelten. Weitere Informationen finden Sie unter Microsoft Defender for App Service in der Microsoft Azure-Dokumentation.

Zukünftige Überlegungen

Integrieren Sie das Scannen von Abhängigkeiten und Sicherheitslücken in Ihre Build- und Deployment-Pipeline, und überwachen Sie Ihre App mithilfe von Microsoft Defender for Cloud im Hinblick auf Konfiguration und Schwachstellenfunde. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Microsoft Defender for App Service.

Die Azure Function-App weist Software-Sicherheitslücken auf

Common Vulnerabilities and Exposures (CVEs) können sich auf Softwarepakete und Abhängigkeiten in Ihrer Function-App auswirken. Bei unkritischen Sicherheitslücken handelt es sich um Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit als Sicherheitslücken mit hoher Priorität. Obwohl sie ein geringeres unmittelbares Risiko darstellen, können Angreifer ungepatchte Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Patchen Sie diese Sicherheitslücken gemäß den bewährten Sicherheitsmethoden, um Ihre Function-App zu schützen.

Behebung: Aktualisieren Sie die betroffenen Abhängigkeiten

Aktualisieren Sie die anfälligen Pakete und Abhängigkeiten auf ihre neuesten sicheren Versionen und stellen Sie die App erneut bereit. Wenn kein Update verfügbar ist, sollten Sie erwägen, die anfällige Komponente zu entfernen oder zu deaktivieren, bis ein Patch veröffentlicht wird. Weitere Informationen finden Sie unter Microsoft Defender for App Service in der Microsoft Azure-Dokumentation.

Die Azure Function-App enthält schädliche Softwarepakete

Bösartige Pakete sind Softwarekomponenten, die schädlichen Code enthalten, der die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten gefährden soll. Bösartige Pakete stellen eine aktive und kritische Bedrohung für Ihre Function-App dar, da Angreifer den Schadcode automatisch ausführen können, ohne eine separate Sicherheitslücke auszunutzen. Entfernen Sie bösartige Pakete gemäß den bewährten Sicherheitsmethoden, um Ihre Function-App vor potenziellen Angriffen zu schützen.

Problembehebung: Untersuchen und entfernen Sie bösartige Pakete

Überprüfen Sie die Funddetails, um die betroffenen Pakete zu identifizieren, entfernen Sie sie aus Ihren Projektabhängigkeiten, erstellen Sie sie aus einer vertrauenswürdigen Quelle neu und stellen

Sie die App erneut bereit. Überprüfen Sie nach der Behebung Ihrer Abhängigkeiten die Lieferkette, um sicherzustellen, dass keine damit verbundenen schädlichen Komponenten mehr vorhanden sind. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Microsoft Defender for App Service.

Behebung von Risiken für Azure Container-Apps

AWS Security Hub kann Risikoprüfungen für Azure Container-Apps generieren.

Auf der Security Hub-Konsole werden die Azure Container-App, die an einer Gefahrenfeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure Container-Apps
  - Die Azure Container-App enthält Klartext-Anmeldeinformationen in Umgebungsvariablen
  - Die Azure Container-App verfügt über eine offene Netzwerksicherheitsgruppe
  - Die Azure Container-App verfügt über eine verwaltete Identität, die nicht den Regeln der geringsten Rechte folgt

- Der Rolle, die der Azure Container-App zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen
- Merkmale der Erreichbarkeit für Azure-Container-Apps
  - Die Azure Container-App ist über das Internet erreichbar

Fehlkonfigurationsmerkmale für Azure Container-Apps

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Container-Apps und empfohlene Korrekturmaßnahmen.

Die Azure Container-App enthält Klartext-Anmeldeinformationen in Umgebungsvariablen

Die Container-App übergibt geheime Daten wie Verbindungszeichenfolgen, API-Schlüssel oder Passwörter als Klartext-Umgebungsvariablen an den Container. Konfiguration, Protokolle oder ein kompromittierter Container können Klartext-Anmeldeinformationen in Umgebungsvariablen preisgeben, sodass ein Angreifer sie für den Zugriff auf andere Systeme wiederverwenden kann. Speichern Sie vertrauliche Werte gemäß den Standardsicherheitsprinzipien als Geheimnisse und referenzieren Sie sie, anstatt sie in Klartext einzubetten.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Verschieben Sie Anmeldeinformationen in geheime Daten

Ersetzen Sie Klartext-Umgebungsvariablenwerte durch geheime Container-Apps oder durch Referenzgeheimnisse, die in Azure Key Vault gespeichert sind. Aktualisieren Sie den Container, um die Werte aus diesen geheimen Referenzen zu lesen. Rotieren Sie alle Anmeldeinformationen, die zuvor im Klartext verfügbar waren. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Verwalten von Geheimnissen in Azure Container Apps.

Verwenden Sie nach Möglichkeit eine verwaltete Identität

Verwenden Sie für Verbindungen zu Azure-Diensten, die dies unterstützen, die verwaltete Identität der Container-App, anstatt überhaupt ein Geheimnis zu speichern. Weitere Informationen finden Sie unter Verwaltete Identitäten in Azure Container Apps in der Microsoft Azure-Dokumentation.

Die Azure Container-App verfügt über eine offene Netzwerksicherheitsgruppe

Die Netzwerksicherheitsgruppe, die die Umgebung der Container-App schützt, enthält Regeln, die den uneingeschränkten Zugriff von jeder Quelle aus ermöglichen (z. B. eine Quelle von

Any oder`0.0.0.0/0`). Eine offene Netzwerksicherheitsgruppe setzt die Umgebung der Container-App einem unbefugten Zugriff aus dem Internet aus. Beschränken Sie die Regeln für Netzwerksicherheitsgruppen gemäß den Standardsicherheitsprinzipien auf die spezifischen IP-Adressen, Ports und Protokolle, die Ihre Arbeitslast benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Schränken Sie die Regeln für Netzwerksicherheitsgruppen ein

Überprüfen Sie die Netzwerksicherheitsgruppe, die dem Subnetz der Container-App-Umgebung zugeordnet ist, und ändern oder entfernen Sie Regeln, die uneingeschränkten Zugriff ermöglichen. Ersetzen Sie eine breite Quelle, z. B. Any durch die spezifischen vertrauenswürdigen Bereiche, die Ihre Arbeitslast benötigt. Weitere Informationen finden Sie unter Netzwerke in Azure Container Apps in der Microsoft Azure-Dokumentation.

Legen Sie IP-Eingangsbeschränkungen fest

Konfigurieren Sie zusätzlich zu den Regeln für Netzwerksicherheitsgruppen im Umgebungssubnetz die IP-Eingangsbeschränkungen für die Container-App selbst, um eingehenden Datenverkehr nach IP-Adressbereich zuzulassen oder abzulehnen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Einrichten von IP-Eingangsbeschränkungen in Azure Container Apps.

Die Azure Container-App verfügt über eine verwaltete Identität, die nicht den Regeln der geringsten Rechte folgt

Die Container-App verfügt über eine verwaltete Identität, der mehr Zugriff gewährt wird, als für den Workload erforderlich ist. Eine überprivilegierte verwaltete Identität erweitert den Explosionsradius, wenn die Container-App kompromittiert wird, da ein Angreifer mit allen Berechtigungen der Identität handeln kann. Gewähren Sie der Identität gemäß den Standardsicherheitsprinzipien nur die Berechtigungen, die die Arbeitslast benötigt, und zwar im engsten Umfang.

Problembehebung: Ordnen Sie der verwalteten Identität die geringsten Rechte zu

Prüfen Sie die Rollenzuweisungen, die der verwalteten Identität der Container-App gewährt wurden, und entfernen Sie alle, die nicht erforderlich sind. Weisen Sie die integrierte Rolle mit den geringsten Rechten im engsten Umfang (Ressource oder Ressourcengruppe) zu, der Ihren Anforderungen entspricht. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Methoden für Azure RBAC.

Der Rolle, die der Azure Container-App zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen

Der verwalteten Identität, die der Container-App zugeordnet ist, ist eine administrative Rollenzuweisung (z. B. `Owner` oder`Contributor`) mit einem breiten Geltungsbereich zugewiesen. Diese Zuweisung gewährt in der Regel Berechtigungen, die weit über das hinausgehen, was die Arbeitslast erfordert. Wenn die Container-App kompromittiert ist, kann ein Angreifer diese übermäßigen Berechtigungen nutzen, um sich quer durch Ihre Umgebung zu bewegen, auf Daten zuzugreifen oder Ressourcen zu manipulieren. Gewähren Sie gemäß den Standardsicherheitsprinzipien die geringsten Rechte, indem Sie nur die Berechtigungen zuweisen, die die App benötigt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um diesem Risiko zu begegnen:

Überprüfen und identifizieren Sie die administrativen Rollenzuweisungen

Überprüfen Sie im Azure-Portal die Rollenzuweisungen für die Identität, die der Container-App zugeordnet ist. Suchen Sie nach privilegierten Administratorrollen wie`Owner`, oder `ContributorUser Access Administrator`, und nach benutzerdefinierten Rollen, in deren `Actions` Rollen ein Platzhalterzeichen (`*`) verwendet wird. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure-Rollenzuweisungen auflisten.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie administrative Rollenzuweisungen durch die integrierte Rolle mit den geringsten Rechten, die nur die Berechtigungen gewährt, die die App benötigt, und weisen Sie sie im engsten Umfang zu, der Ihren Anforderungen entspricht. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Methoden für Azure RBAC.

Merkmale der Erreichbarkeit für Azure-Container-Apps

Im Folgenden finden Sie Erreichbarkeitsmerkmale für Azure-Container-Apps und empfohlene Abhilfemaßnahmen.

Die Azure Container-App ist über das Internet erreichbar

Die Container-App ist über das öffentliche Internet erreichbar, entweder weil externer Zugriff aktiviert ist (auf eingestellt `ingress.external` ist`true`) oder weil ihre Umgebung eine öffentliche IP-Adresse hat. Die öffentliche Erreichbarkeit erhöht die Angriffsfläche der Container-App und setzt sie unerlaubten Anfragen aus. Deaktivieren Sie externen Zugriff gemäß den

Standardsicherheitsprinzipien, wenn er nicht erforderlich ist, verwenden Sie eine interne Umgebung oder platzieren Sie die App hinter einem kontrollierten, authentifizierten Zugangspunkt.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Schränken Sie externen Zugriff ein oder entfernen Sie ihn

Stellen Sie den Eingang auf intern ein, wenn die App nur von Ihrem virtuellen Netzwerk oder Ihrer virtuellen Umgebung aus erreicht werden muss. Wenn öffentlicher Zugriff erforderlich ist, schränken Sie ihn mit IP-Zugangsbeschränkungen ein. Stellen Sie der App ein Gateway wie Azure Application Gateway oder Azure Front Door zur Verfügung.

Diese Gateways bieten Authentifizierung und eine Firewall für Webanwendungen. Weitere Informationen finden Sie unter Ingress in Azure Container Apps in der Microsoft Azure-Dokumentation.

Verwenden Sie eine interne Umgebung

Um die Zuweisung einer öffentlichen IP-Adresse zu vermeiden, stellen Sie die Container-App in einer internen (in ein virtuelles Netzwerk integrierten) Umgebung bereit, die eine private IP-Adresse verwendet, und legen Sie nur die Endpunkte offen, die öffentlich sein müssen, über einen kontrollierten Zugangspunkt. Weitere Informationen finden Sie unter Netzwerke in Azure Container Apps in der Microsoft Azure-Dokumentation.

Für öffentlichen Zugriff sind HTTPS und Authentifizierung erforderlich

Wenn der eingehende Zugriff öffentlich bleiben muss, deaktivieren Sie unsichere Verbindungen (`allowInsecure`auf gesetzt`false`), sodass der Datenverkehr nur über HTTPS abgewickelt wird. Aktivieren Sie die integrierte Authentifizierungsfunktion mit Microsoft Entra ID, damit nicht authentifizierte Anfragen abgelehnt werden. Weitere Informationen finden Sie unter Authentifizierung und Autorisierung in Azure Container Apps in der Microsoft Azure-Dokumentation.

Behebung von Risiken für Azure Kubernetes Service-Cluster

AWS Security Hub kann Risikoprüfungen für Azure Kubernetes Service (AKS) -Cluster generieren.

Auf der Security Hub-Konsole werden der AKS-Cluster, der an einer Gefahrenfeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure Kubernetes Service-Cluster
  - Auf dem Azure Kubernetes Service-Cluster wird eine Kubernetes-Version ausgeführt, die nicht unterstützt wird
  - Der Azure Kubernetes Service-Cluster verfügt über unverschlüsselte Kubernetes-Geheimnisse
- Erreichbarkeitsmerkmale für Azure Kubernetes Service-Cluster
  - Der Azure Kubernetes Service-Cluster ermöglicht den öffentlichen Zugriff

Fehlkonfigurationsmerkmale für Azure Kubernetes Service-Cluster

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Kubernetes Service-Cluster und empfohlene Behebungsschritte.

Auf dem Azure Kubernetes Service-Cluster wird eine Kubernetes-Version ausgeführt, die nicht unterstützt wird

Auf dem AKS-Cluster wird eine Kubernetes-Version ausgeführt, die von Microsoft nicht mehr unterstützt wird. Nicht unterstützte Kubernetes-Versionen erhalten keine Sicherheitspatches und Bugfixes mehr, wodurch bekannte Sicherheitslücken in der Steuerungsebene und den Knotenkomponenten nicht behoben werden und der Cluster einem Angriff ausgesetzt ist. Halten Sie

sich an die bewährten Sicherheitsmethoden und verwenden Sie für den Cluster eine unterstützte Kubernetes-Version.

Behebung: Führen Sie ein Upgrade auf eine unterstützte Kubernetes-Version durch

Führen Sie ein Upgrade der Cluster-Steuerungsebene und der Knotenpools auf eine unterstützte Kubernetes-Version durch. Da Nebenversionen nicht übersprungen werden können, führen Sie das Upgrade nacheinander durch jede Nebenversion durch und wenden Sie den neuesten Patch an. Überprüfen Sie vor dem Upgrade die wichtigsten Änderungen für jede Version.

Erwägen Sie, automatische Upgrades zu aktivieren, um auf dem neuesten Stand zu bleiben. Weitere Informationen finden Sie unter Unterstützte Kubernetes-Versionen in AKS in der Microsoft Azure-Dokumentation.

Der Azure Kubernetes Service-Cluster verfügt über unverschlüsselte Kubernetes-Geheimnisse

Standardmäßig speichert der Cluster Kubernetes-Geheimnisse im etcd-Datenspeicher ohne Verschlüsselung durch einen vom Kunden kontrollierten Schlüssel. Ohne Verschlüsselung im Ruhezustand mithilfe eines Schlüsselverwaltungsdienstes kann jeder, der Zugriff auf die zugrunde liegenden etcd-Daten erhält, vertrauliche geheime Werte wie Anmeldeinformationen und Token lesen. Aktivieren Sie die KMS-etcd-Verschlüsselung gemäß den bewährten Datenschutzmethoden, sodass Kubernetes-Geheimnisse im Ruhezustand mit einem Schlüssel in Azure Key Vault verschlüsselt werden.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Aktivieren Sie die KMS- und etcd-Verschlüsselung

Konfigurieren Sie den Cluster so, dass er die Key Management Service (KMS) etcd-Verschlüsselung mit einem in Azure Key Vault gespeicherten Schlüssel verwendet. Gewähren Sie dem Cluster die Berechtigungen zum Verschlüsseln und Entschlüsseln der Clusteridentität für den Schlüssel. Re-encrypt vorhandene Geheimnisse, nachdem Sie die Funktion aktiviert haben. Aktivieren Sie den Schutz vor automatischem Löschen und Löschen im Schlüsseltresor, damit der Schlüssel nicht verloren gehen kann. Weitere Informationen finden Sie unter KMS-etcd-Verschlüsselung in AKS in der Microsoft Azure-Dokumentation.

Aktivieren Sie den Soft-Delete- und Löschschutz für den Schlüsseltresor, damit der Schlüssel nicht verloren gehen kann. Weitere Informationen finden Sie unter KMS-etcd-Verschlüsselung in AKS in der Microsoft Azure-Dokumentation.

Speichern Sie Geheimnisse in Azure Key Vault

Um zu vermeiden, dass vertrauliche Werte als Kubernetes-Geheimnisse in etcd gespeichert werden, verwenden Sie den Azure Key Vault-Anbieter für den Secrets Store CSI-Treiber, um Geheimnisse, Schlüssel und Zertifikate aus Azure Key Vault zur Laufzeit in Pods einzubinden. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure Key Vault-Anbieter für den Secrets Store CSI-Treiber.

Erreichbarkeitsmerkmale für Azure Kubernetes Service-Cluster

Im Folgenden finden Sie Erreichbarkeitsmerkmale für Azure Kubernetes Service-Cluster und empfohlene Abhilfemaßnahmen.

Der Azure Kubernetes Service-Cluster ermöglicht den öffentlichen Zugriff

Der API-Server ist der Endpunkt, den Sie für die Kommunikation mit der Kubernetes-Steuerungsebene Ihres Clusters verwenden. Der Cluster ist über das Internet erreichbar, wenn der API-Serverendpunkt öffentlich ist oder wenn Workloads über einen öffentlichen Load Balancer oder Ingress verfügbar gemacht werden. Öffentliche Endpunkte erhöhen Ihre Angriffsfläche und das Risiko eines unbefugten Zugriffs auf Ihren Kubernetes-API-Server. Angreifer können potenziell auf Cluster-Ressourcen zugreifen oder diese ändern und sensible Daten lesen. Beschränken Sie den Zugriff auf den API-Server und die Workloads Ihres Clusters gemäß den bewährten Sicherheitsmethoden auf nur die erforderlichen IP-Bereiche.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieses Risiko zu beheben:

Beschränken Sie den Zugriff auf den API-Server

Verwenden Sie einen privaten Cluster, sodass der API-Server nur von Ihrem virtuellen Netzwerk aus erreichbar ist, oder konfigurieren Sie autorisierte IP-Bereiche, um einzuschränken, welche Quelladressen den öffentlichen API-Serverendpunkt erreichen können. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Private Azure Kubernetes Service-Cluster.

Beschränken Sie die Offenlegung von Workloads in der Öffentlichkeit

Prüfen Sie Dienste, die durch öffentliche Load Balancer oder Ingress gefährdet sind, und schränken Sie die öffentliche Exposition ein oder entfernen Sie sie, wenn dies nicht erforderlich ist. Verwenden Sie interne Load Balancer, Netzwerksicherheitsgruppenregeln und eine Webanwendungs-Firewall an einem kontrollierten Eingangspunkt für Workloads, die über das Internet erreicht werden

müssen. Weitere Informationen finden Sie unter Netzwerkkonzepte für AKS in der Microsoft Azure-Dokumentation.

Behebung von Risiken für Azure Graph-Benutzer

AWS Security Hub kann Bedrohungsergebnisse für Azure Graph-Benutzer generieren.

Auf der Security Hub-Konsole werden der Azure Graph-Benutzer, der an einer Gefahrenfeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ermittlungsdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der GetFindingsV2 Security Hub CSPM-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Das Löschen einer Ressource, die nicht unbedingt erforderlich ist, kann Ihr Risikoprofil und Ihre AWS Kosten reduzieren. Wenn es sich um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu mindern. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziges Expositionsergebnis enthält Probleme, die in mehreren Sanierungsthemen identifiziert wurden. Umgekehrt können Sie ein Expositionsergebnis behandeln und dessen Schweregrad herabsetzen, indem Sie sich nur mit einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von Ihren organisatorischen Anforderungen und Arbeitsbelastungen ab.

> **Note**
>
> Die in diesem Thema bereitgestellten Anleitungen zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen Microsoft Azure-Ressourcen.

Inhalt

- Fehlkonfigurationsmerkmale für Azure Graph-Benutzer
  - Der Rolle, die dem Azure Graph-Benutzer zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen
  - Für den Azure Graph-Benutzer ist MFA nicht aktiviert

Fehlkonfigurationsmerkmale für Azure Graph-Benutzer

Im Folgenden finden Sie Fehlkonfigurationsmerkmale für Azure Graph-Benutzer und empfohlene Korrekturmaßnahmen.

Der Rolle, die dem Azure Graph-Benutzer zugeordnet ist, ist eine Administratorzugriffsrolle zugewiesen

Dem Azure Graph-Benutzer ist eine administrative Azure Role-Based Access Control (Azure RBAC) -Rollenzuweisung zugewiesen, z. B.`Owner`, oder. `Contributor` `User Access Administrator` Die Zuweisung umfasst häufig einen breiten Anwendungsbereich, z. B. eine Abonnement- oder Verwaltungsgruppe. Durch die Zuweisung administrativer Rollen werden weitreichende Rechte gewährt, sodass ein Angreifer ein kompromittiertes Benutzerkonto verwenden kann, um sich in Ihrer Umgebung zu bewegen, auf Daten zuzugreifen oder Ressourcen zu manipulieren. Gewähren Sie gemäß den Standardsicherheitsprinzipien die geringsten Rechte und beschränken Sie die Zuweisung berechtigter Administratorrollen.

Abhilfe

Ergreifen Sie eine oder mehrere der folgenden Maßnahmen, um dieser Gefahr zu begegnen:

Überprüfen und identifizieren Sie die administrativen Rollenzuweisungen

Überprüfen Sie im Azure-Portal die Rollenzuweisungen des Benutzers. Suchen Sie nach privilegierten Administratorrollen wie`Owner`, oder `Contributor``User Access Administrator`, und nach benutzerdefinierten Rollen, in deren `Actions` Rollen ein Platzhalter (`*`) verwendet wird. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Azure-Rollenzuweisungen auflisten.

Implementieren des Zugriffs mit geringsten Berechtigungen

Entfernen Sie unnötige privilegierte Rollenzuweisungen und ersetzen Sie sie durch die integrierte Rolle mit den geringsten Rechten, die im engsten Umfang zugewiesen wird. Bevorzugen Sie Rollen mit bestimmten Funktionen gegenüber privilegierten Administratorrollen. Beschränken Sie die Anzahl der Abonnementinhaber auf ein Minimum — Microsoft empfiehlt, nicht mehr als drei zu verwenden.

Weisen Sie Gruppen und nicht einzelnen Benutzern Rollen zu. Verwenden Sie Microsoft Entra Privileged Identity Management, um privilegierten Rollen eine zeitlich begrenzte Just-in-Time-Aktivierung zu ermöglichen, anstatt Dauerzugriff zu gewähren. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Bewährte Methoden für Azure RBAC.

Für den Azure Graph-Benutzer ist MFA nicht aktiviert

Der Azure Graph-Benutzer kann sich interaktiv ohne Multifaktor-Authentifizierung (MFA) anmelden. Ohne MFA ist ein Konto nur durch ein Passwort geschützt, wodurch es anfällig für Phishing-, Passwortspray- und Credential-Stuffing-Angriffe ist. Ein einziges kompromittiertes Passwort reicht

aus, damit sich ein Angreifer anmelden kann. Erfordern Sie gemäß den Standardsicherheitsprinzipien MFA für alle Benutzer mit interaktiver Anmeldung.

Problembehebung: Multifaktor-Authentifizierung erforderlich

Erfordern Sie MFA für den Benutzer mithilfe einer Microsoft Entra-Richtlinie für bedingten Zugriff. Um eine breite Abdeckung zu gewährleisten, aktivieren Sie Sicherheitsstandards oder eine Richtlinie für bedingten Zugriff, die MFA für alle Benutzer vorschreibt. Priorisieren Sie eine spezielle Richtlinie für Administratoren.

Verwenden Sie nach Möglichkeit Methoden, die gegen Phishing resistent sind — z. B. FIDO2-Sicherheitsschlüssel, Hauptschlüssel oder Windows Hello for Business — mithilfe einer Authentifizierungsstärke für bedingten Zugriff. Vermeiden Sie es, phishingfähige Methoden wie SMS oder Spracheingabe zuzulassen. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation unter Planen einer Bereitstellung der Multifaktor-Authentifizierung.

Erkenntnisse über ungenutzte Zugriffe in Security Hub verstehen

Security Hub verwendet IAM Access Analyzer, um ungenutzte IAM-Berechtigungen, Rollen, Zugriffsschlüssel und Passwörter in Ihrem Konto zu identifizieren. Diese Ergebnisse helfen Ihnen dabei, die bewährte Sicherheitsmethode des Zugriffs mit den geringsten Rechten zu implementieren, indem IAM-Prinzipale und -Berechtigungen hervorgehoben werden, die nicht aktiv genutzt werden. Diese Funktion wird allen Security Hub-Kunden ohne zusätzliche Kosten zur Verfügung gestellt.

So funktioniert die Analyse ungenutzter Zugriffe

Wenn Sie Security Hub aktivieren, erstellt der Dienst automatisch einen dienstverknüpften IAM Access Analyzer in Ihrem Konto. Dieser Analyzer bewertet alle IAM-Prinzipale (Rollen und Benutzer) anhand der AWS CloudTrail Aktivitätsdaten, um festzustellen, welche Principals und Berechtigungen innerhalb eines 90-tägigen Lookback-Zeitraums nicht verwendet wurden. Der Lookback-Zeitraum ist nicht konfigurierbar.

IAM Access Analyzer bewertet alle aktiven Ergebnisse alle 24 Stunden neu. Wenn ein zuvor nicht verwendeter Principal oder eine zuvor ungenutzte Genehmigung aktiv wird, wird das entsprechende Ergebnis automatisch behoben.

Der ungenutzte Access Analyzer wird im Osten der USA (Nord-Virginia) ausgeführt, da es sich bei IAM um einen globalen Dienst handelt. Security Hub repliziert die Ergebnisse in alle Regionen, in denen Sie Security Hub aktiviert haben. Sie müssen Security Hub in den USA Ost (Nord-Virginia) nicht aktivieren, damit der Analyzer ausgeführt werden kann.

Ungenutzte Typen zur Zugriffsermittlung

Security Hub generiert vier Arten von ungenutzten Zugriffsergebnissen:

Ergebnistyp	Description	Evaluierte Ressource
Ungenutzte IAM-Rolle	Eine IAM-Rolle, die innerhalb der 90-Tage-Lookback-Frist nicht übernommen wurde.	IAM role (IAM-Rolle)
UnusedIAM UserAccessKey	Ein IAM-Benutzerzugriffsschlüssel, der innerhalb des 90-Tage-Lookback-Zeitraums nicht zum Signieren von API-Anfragen verwendet wurde.	IAM-Benutzer
UnusedIAM UserPassword	Ein IAM-Benutzerkennwort, das innerhalb des 90-Tage-Lookback-Zeitraums nicht für die Konsolenanmeldung verwendet wurde.	IAM-Benutzer
UnusedPermission	Spezifische IAM-Aktionen, die einer Rolle oder einem Benutzer gewährt wurden, aber nicht innerhalb des 90-tägigen Lookback-Zeitraums aufgerufen wurden.	IAM-Rolle oder IAM-Benutzer

Service-linked Analysator

Der IAM Access Analyzer, den Security Hub erstellt, ist ein dienstgebundener Analyzer. Sie können ihn in der IAM Access Analyzer-Konsole anzeigen, aber Sie können ihn nicht ändern oder löschen, solange Security Hub aktiviert ist.

Wenn Sie Security Hub in allen Regionen deaktivieren, wird der mit dem Service verknüpfte Analyzer automatisch gelöscht. Wenn das automatische Löschen fehlschlägt, können Sie den Analyzer löschen, indem Sie den IAM Access `DeleteServiceLinkedAnalyzer` Analyzer-API-Vorgang aufrufen. Dieser Vorgang ist erst erfolgreich, nachdem Security Hub für Ihr Konto vollständig deaktiviert wurde.

Der Service Linked Analyzer ist von allen vom Kunden verwalteten Analyzern getrennt, die Sie möglicherweise unabhängig in IAM Access Analyzer erstellt haben. Das Erstellen oder Löschen von kundenverwalteten Analyzern wirkt sich nicht auf den Service-Linked Analyzer aus und umgekehrt.

Ergebnisse ungenutzter Zugriffe anzeigen

Ergebnisse ungenutzter Zugriffe werden in der Security Hub-Konsole zusammen mit anderen Security Hub-Ergebnissen angezeigt. Sie können die Ergebnisse nach Typ filtern, um nur ungenutzte Zugriffsergebnisse anzuzeigen. Ergebnisse ungenutzter Zugriffe werden im Open Cybersecurity Schema Framework (OCSF) formatiert, dem gleichen Format, das von allen Security Hub-Ergebnissen verwendet wird.

Wenn Sie bei UnusedPermission Ergebnissen einige ungenutzte Berechtigungen aus der übermäßig freizügigen Richtlinie entfernen, aber nicht alle, schließt Security Hub das vorhandene Ergebnis und erstellt ein neues Ergebnis für die überarbeitete Richtlinie, falls diese immer noch zu freizügig ist.

Ergebnisse für ungenutzte Zugriffe sind auch über die IAM Access Analyzer-Konsole zugänglich. Nicht verwendete Zugriffsergebnisse in der IAM Access Analyzer-Konsole sind schreibgeschützt und nur in der Region USA Ost (Nord-Virginia) sichtbar.

Ungenutzter Zugriff auf Expositionsergebnisse

Ungenutzte Zugriffsinformationen können als kontextuelle Merkmale in den Sicherheitsergebnissen von Security Hub auftauchen. Wenn eine IAM-Rolle, die einer Ressource zugeordnet ist, über ungenutzte Berechtigungen verfügt, wird dies in der Bedrohungsermittlung als zusätzlicher Kontext berücksichtigt. Dies hilft Ihnen, den potenziellen Explosionsradius einer Sicherheitslücke zu verstehen — eine Ressource mit einer überprivilegierten IAM-Rolle stellt ein höheres Risiko dar als eine Ressource mit Berechtigungen mit geringsten Rechten.

Die folgenden Ressourcentypen können in ihren Gefährdungsergebnissen ungenutzte Zugriffskontextmerkmale aufweisen:

- Amazon Elastic Compute Cloud-Instanzen
- AWS Lambda Funktionen
- Dienste von Amazon Elastic Container Service
- Amazon Elastic Kubernetes Service-Cluster
- IAM-Benutzer (direkt)

Weitere Informationen zu Expositionsergebnissen finden Sie unterErkenntnisse zu Sicherheitsrisiken in Security Hub.

Politische Empfehlungen für ungenutzte Berechtigungen

Für die UnusedPermission Ergebnisse kann Security Hub Richtlinienempfehlungen zum Thema „Least Privilege“ erstellen. Aus diesen Empfehlungen geht hervor, dass es sich um eine erweiterte Ersatzrichtlinie handelt, bei der nur die Berechtigungen beibehalten werden, die Ihr Auftraggeber tatsächlich verwendet. Weitere Informationen finden Sie unter Generierung von politischen Empfehlungen für ungenutzte Zugriffsergebnisse.

Preisgestaltung

Der mit dem Service verbundene IAM Access Analyzer wird allen Security Hub-Kunden ohne zusätzliche Kosten zur Verfügung gestellt. Der Analyzer oder ungenutzte Zugriffsergebnisse werden Ihnen nicht separat in Rechnung gestellt.

Generierung von politischen Empfehlungen für ungenutzte Zugriffsergebnisse

Wenn ungenutzte Berechtigungen gefunden werden, kann Security Hub Empfehlungen für Richtlinien mit den geringsten Rechten erstellen, die Ihnen eine erweiterte Ersatzrichtlinie aufzeigen. Die Empfehlung bewertet jede dem IAM-Prinzipal zugeordnete Richtlinie und generiert eine Ersatzrichtlinie, die nur die Berechtigungen beibehält, die der Prinzipal tatsächlich verwendet hat. Diese Funktion wird allen Security Hub-Kunden ohne zusätzliche Kosten zur Verfügung gestellt.

So funktionieren politische Empfehlungen

Die Generierung von Richtlinienempfehlungen ist ein asynchroner Vorgang. Um eine Empfehlung zu generieren und abzurufen:

1. Rufen Sie mithilfe des `GetFindingsV2` API-Vorgangs die Suche nach ungenutzten Berechtigungen von Security Hub ab. Notieren Sie sich das `metadata.uid` Feld aus dem Ergebnis.
2. Rufen Sie `GenerateRecommendedPolicyV2` mit den Ergebnissen an`metadata.uid`. Dadurch wird die Generierung der Empfehlung initiiert, die in der Regel innerhalb von 20 Sekunden abgeschlossen ist.
3. Fragen Sie `GetRecommendedPolicyV2` mit derselben ab, `metadata.uid` bis das `status` Feld zurückkehrt`SUCCEEDED`.

4. Die Antwort enthält einen oder mehrere Empfehlungsschritte. In jedem Schritt wird entweder `CREATE_POLICY` (eine `recommendedAction` erweiterte Ersatzrichtlinie erstellen und anhängen) oder `DETACH_POLICY` (die ursprüngliche Richtlinie mit übermäßigen Rechten entfernen) angegeben. Bei `CREATE_POLICY` Schritten umfasst die Antwort sowohl JSON als auch `existingPolicy` JSON, sodass Sie sie vergleichen `recommendedPolicy` können.

Sie müssen `GenerateRecommendedPolicyV2` vor dem Anruf anrufen, `GetRecommendedPolicyV2` wenn für dieses Ergebnis noch keine Empfehlung generiert wurde.

Wer kann Empfehlungen generieren

Sowohl der Kontoinhaber als auch delegierte Administratoren können diese API-Operationen aufrufen:

- Kontoinhaber können Empfehlungen für ungenutzte Berechtigungen in ihrem eigenen Konto generieren und einsehen.
- Delegierte Administratoren können Empfehlungen für ungenutzte Berechtigungen aller Mitgliedskonten innerhalb ihrer Organisation erstellen und einsehen.

Wenn Sie kein delegierter Administrator sind und das Ergebnis zu einem anderen Konto gehört, gibt der API-Vorgang einen `AccessDeniedException` Fehler zurück.

Lebenszyklus der Empfehlung

- Empfehlungen werden 90 Tage lang zwischengespeichert und bleiben verfügbar, solange das Ergebnis aktiv (nicht geschlossen) ist. Ein `GenerateRecommendedPolicyV2` mehrmaliger Aufruf macht den Cache jedoch ungültig und ein neuer Job wird gestartet, der die zwischengespeicherte Richtlinie ersetzt. Rufen Sie `GenerateRecommendedPolicyV2` nur einmal pro Ergebnis auf.
- Die Empfehlung folgt dem Muster „Trennen und Anhängen“. Ihre vorhandenen IAM-Richtlinien werden dadurch nicht geändert. Sie überprüfen die empfohlene Richtlinie und wenden sie manuell in der IAM-Konsole oder über die IAM-API an.
- Wenn das Problem behoben ist (z. B. weil die zuvor ungenutzten Berechtigungen jetzt verwendet werden), ist die Empfehlung nicht mehr verfügbar.

Fehlerfälle

Die API-Operationen geben in den folgenden Situationen Fehler zurück:

- Das Ergebnis wurde behoben — `InvalidInputException` (HTTP 400).
- Das Ergebnis ist kein Ergebnis ungenutzter Berechtigungen — `InvalidInputException` (HTTP 400).
- Der IAM-Prinzipal wurde mithilfe des IAM Identity Center-Berechtigungssatzes erstellt. Richtlinien für Berechtigungssatz-Prinzipale können nicht direkt geändert werden. Die Empfehlung gibt einen `FAILED` Status mit einer Erklärung zurück.
- Der Anrufer ist kein delegierter Administrator und das Ergebnis gehört zu einem anderen Konto — `AccessDeniedException` (HTTP 403).
- Es wurde noch keine Empfehlung generiert und Sie rufen an, `GetRecommendedPolicyV2` ohne vorher anzurufen `GenerateRecommendedPolicyV2` — `ResourceNotFoundException` (HTTP 404).

Verwenden der Konsole

In der Security Hub-Konsole können Sie eine Richtlinienempfehlung generieren, indem Sie nach ungenutzten Berechtigungen suchen und die Registerkarte Behebung auswählen. Während die Empfehlung erstellt wird, zeigt die Konsole einen Loading Spinner an. Wenn die Empfehlung fertig ist, können Sie „Vorschau“ wählen, um einen direkten Vergleich zwischen Ihrer aktuellen Richtlinie und dem empfohlenen Ersatz mit den geringsten Rechten zu sehen. Sie können die empfohlene Richtlinie im JSON-Format kopieren.

API-Referenz

- GenerateRecommendedPolicyV2— Initiiert die asynchrone Generierung einer Richtlinienempfehlung nach dem Prinzip der geringsten Rechte für die Suche nach ungenutzten Berechtigungen. Nimmt die Ergebnisse als Eingabe an. `metadata.uid` Gibt bei Erfolg HTTP 200 mit leerem Text zurück.
- GetRecommendedPolicyV2— Ruft die generierte Richtlinienempfehlung ab. Nimmt die Ergebnisse `metadata.uid` als Eingabe an. Unterstützt die Paginierung mit `maxResults` (1—100) und `nextToken` Parametern. Gibt den Empfehlungsstatus (`IN_PROGRESS`,`SUCCEEDED`, oder`FAILED`), die Empfehlungsschritte, den Ressourcen-ARN und alle Fehler zurück.

Eine ausführliche API-Dokumentation finden Sie in der Security Hub-API-Referenz.

Netzwerkscannen im Security Hub

Netzwerk-Scanning ist eine optionale Funktion von Security Hub, die aktive Netzwerkerreichbarkeitstests für Ihre Cloud-Ressourcen durchführt. Control-plane Bei der Analyse werden Sicherheitsgruppen, Network Access Control Lists (NACLs) und Routing-Tabellen ausgewertet, um festzustellen, welche Bereiche erreichbar sein könnten. Network Scanning geht noch einen Schritt weiter und erkennt, was tatsächlich erreichbar ist. Es untersucht Ihre Ressourcen von außerhalb Ihrer Konten, um offene Ports und laufende Dienste zu identifizieren.

Alle Scans stammen AWS von eigenen IP-Adressen und beantworten zwei Fragen: Ist diese Ressource über das Internet erreichbar? Wenn erreichbar, was läuft? Network Scanning veröffentlicht Ergebnisse als eigenständige OCSF-Ergebnisse zusammen mit Scannachweisen in Security Hub.

Unterstützte Ressourcentypen

Network Scanning unterstützt die folgenden Ressourcentypen.

Cloud-Anbieter	Ressourcentyp
AWS	EC2-Instanz (mit öffentlicher IP)
AWS	Elastische IP (EIP)
AWS	Network Load Balancer (NLB)
AWS	Anwendungs-Load Balancer (ALB)
AWS	Klassischer Load Balancer (CLB)
Azure	Öffentliche IP-Adresse

> **Note**
>
> Network Scanning scannt jeden Ressourcentyp unabhängig. Bei Load Balancern löst Network Scanning den DNS-Namen auf und scannt ihn. Network Scanning scannt nur

einzelne EC2-Instances hinter einem Load Balancer, wenn sie über eine eigene öffentliche IP oder EIP verfügen.

Netzwerk-Scannen aktivieren

Um das Scannen von Netzwerken zu aktivieren, muss Security Hub in Ihrem Konto aktiviert sein. Sie können das Netzwerkscannen über eine Konfigurationsrichtlinie oder für einzelne Konten aktivieren.

Organisationskonten (empfohlen) — Aktivieren Sie das Netzwerkscannen für alle Konten und Regionen Ihrer Organisation, indem Sie eine Konfigurationsrichtlinie erstellen oder bearbeiten. Weitere Informationen zum Bearbeiten einer Konfigurationsrichtlinie finden Sie unter Bearbeiten einer Konfigurationsrichtlinie. Wenn das Netzwerkscannen über eine Konfigurationsrichtlinie aktiviert ist, können Mitgliedskonten die Funktion nicht deaktivieren.

Individuelle Konten — Für Konten, die nicht durch eine Konfigurationsrichtlinie verwaltet werden, können Sie den Netzwerk-Scan mit einer der folgenden Methoden aktivieren.

> **Note**
>
> Durch die Aktivierung von Network Scanning autorisieren Sie Security Hub, aktive Netzwerkscans gegen Ressourcen in Ihren AWS Umgebungen und Azure-Umgebungen durchzuführen. Dazu gehören TCP-Port-Verbindungsversuche, Anwendungs- und Protokollidentifikation sowie die Erfassung von Dienstbannern, HTTP-Headern und TLS-Zertifikatsmetadaten.

Security Hub console

Um das Scannen im Netzwerk zu aktivieren

1. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Allgemeine Einstellungen aus.
3. Suchen Sie den Abschnitt Netzwerkscannen.
4. Wählen Sie Enable (Aktivieren) aus.
5. Bestätigen Sie die Autorisierung, um mit dem aktiven Netzwerkscannen fortzufahren.

Security Hub API

Rufen Sie die `EnableSecurityHubFeatureV2` API mit dem Funktionsnamen `NETWORK_SCANNING` auf.

> **Note**
>
> Wenn Sie diese API aufrufen, wenn das Netzwerkscannen bereits aktiviert ist, wird eine Antwort von 200 zurückgegeben. Der Dienst behält den `UpdatedAt` Zeitstempel der ursprünglichen Aktivierung bei.

AWS CLI

Führen Sie den folgenden Befehl aus, um den Netzwerk-Scan zu aktivieren:

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

So funktioniert das Scannen im Netzwerk

Nachdem Sie den Netzwerk-Scan aktiviert haben, passiert Folgendes:

- Der Netzwerk-Scan scannt vorhandene Ressourcen innerhalb von etwa 24 Stunden nach der Aktivierung der Funktion.
- Network Scanning scannt neue Ressourcen, kurz nachdem Security Hub eine Benachrichtigung über die erstellte Ressource erhalten hat.
- Network Scanning scannt Ressourcen erneut, wenn bestimmte geeignete Änderungen an der Steuerungsebene an einer zum Scannen geeigneten Ressource vorgenommen werden.
- Beim Netzwerk-Scannen werden aktive Ressourcen etwa alle 12 Stunden erneut gescannt, um Änderungen an der Erreichbarkeit zu erkennen.

Kurzlebige oder kurzlebige Ressourcen werden möglicherweise nicht gescannt, bevor sie beendet werden.

Ergebnisse von Netzwerk-Scans

Network Scanning veröffentlicht die Ergebnisse im Open Cybersecurity Schema Framework (OCSF) - Format unter Verwendung der AWS OCSF-Erweiterung. Sie werden zusammen mit anderen Security

Hub-Ergebnissen angezeigt. Network Scanning ermittelt, ob eine Ressource erreichbare Ports hat oder nicht. Wenn für einen unterstützten Ressourcentyp kein Ergebnis gefunden wurde, hat Network Scanning die Ressource noch nicht gescannt.

Ergebnisse für erreichbare Ports

Jedes Ergebnis steht für einen einzelnen erreichbaren Port auf einer bestimmten Kombination aus Ressource und Adresse. Der `port_scan_result_list` Abschnitt eines OCSF-Ergebnisses enthält die Scanergebnisse. Die folgenden Beispiele zeigen Informationen, die für eine erreichbare Ressource zurückgegeben wurden:

```
"port_scan_result_list": [
    {
      "port_info": {
        "port": 6379,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1,
      "svc_name": "redis"
    }
],
```

```
"port_scan_result_list": [
    {
      "http_response": {
        "code": 200,
        "content_type": "text/html; charset=UTF-8",
        "http_headers": [
          {
            "name": "Server",
            "value": "Apache/2.4.68 (Amazon Linux)"
          },
          {
            "name": "Content-Type",
            "value": "text/html; charset=UTF-8"
          }
        ],
```

```
        "latency": 124
      },
      "port_info": {
        "port": 8080,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1
    }
  ],
```

Informative Ergebnisse für keine offenen Ports

Beim Netzwerkscannen wird ein Ergebnis generiert, wenn keine offenen Ports auf einer Ressource erkannt werden. Dieses Ergebnis hat einen Schweregrad von `Informational` und erfordert keine Maßnahmen. Es bestätigt, dass Network Scanning die Ressource gescannt hat.

Die Informationssuche bleibt in Security Hub geöffnet, bis Sie die Ressource löschen oder bis der Netzwerk-Scan offene Ports auf der Ressource erkennt. Wenn der Netzwerk-Scan offene Ports auf einer Ressource mit einem informativen Ergebnis identifiziert, wird das Informationssuchen geschlossen. Anschließend wird für jeden offenen Port ein Ergebnis erstellt.

Informationen über keine offenen Ports beziehen sich auf die Ports, die Network Scanning derzeit unterstützt. Eine Liste der unterstützten Ports finden Sie unterthe section called “Unterstützte Anschlüsse”.

Suchen nach Ereignissen im Lebenszyklus

In der folgenden Tabelle wird der Lebenszyklus einer Netzwerkscanning-Entdeckung beschrieben.

Veranstaltung	Was passiert
Keine offenen Ports erkannt	Beim Netzwerkscannen wird ein `Informational` Ergebnis erstellt, für das keine Aktion erforderlich ist
Bei der Suche nach Informationen wurden offene Ports auf der Ressource erkannt	Network Scanning schließt die Informationssuche und erstellt eine Suche für jeden offenen Port

Veranstaltung	Was passiert
Der Port wurde zuerst als erreichbar erkannt	Network Scanning erstellt und veröffentlicht ein neues Ergebnis
Der Port ist beim erneuten Scannen immer noch erreichbar (keine Änderung)	Beim Netzwerk-Scannen wird das Ergebnis regelmäßig aktualisiert
Der Port ist immer noch erreichbar, aber die Beweise haben sich geändert	Network Scanning veröffentlicht das Ergebnis erneut mit aktualisierten Beweisen
Port ist nicht mehr erreichbar	Die Suche bleibt offen, bis beim nächsten erneuten Scan bestätigt wird, dass der Port nicht erreichbar ist
Ressource wurde beendet oder gelöscht	Network Scanning schließt alle Ergebnisse für die Ressource ab, indem das `activity_name` Attribut auf gesetzt wird `Close`
Die IP-Adresse wurde aus der Ressource entfernt	Der Netzwerk-Scan schließt die Ergebnisse für diese bestimmte IP ab
Netzwerk-Scannen ist deaktiviert	Das Scannen im Netzwerk liefert keine neuen Ergebnisse. Bestehende Ergebnisse bleiben bestehen, bis sie veraltet sind
Security Hub ist deaktiviert	Sie haben keinen Zugriff mehr auf Ergebnisse

Wenn ein Port zeitweise erreichbar ist, basiert das Netzwerk-Scannen auf der Grundlage positiver Beweise zum Zeitpunkt des Scans. Nachdem Sie ein Problem behoben haben (z. B. indem Sie eine Firewallregel schließen oder einen Dienst beenden), schließt der Netzwerk-Scan das Ergebnis beim nächsten Scan.

Wenn Sie den Netzwerk-Scan deaktivieren, werden die Ergebnisse nicht sofort geschlossen. Bestehende Ergebnisse bleiben sichtbar, bis sie den normalen Security Hub-Suchzyklus durchlaufen.

> **Note**
>
> Wenn Sie einer Amazon EC2-Instance eine Elastic IP-Adresse (EIP) zuordnen, generiert Network Scanning Ergebnisse für die EIP-Ressource. Die EIP ist die IP-Ressource der

obersten Ebene, der die Adresse gehört. Bei Network Load Balancer (NLB) -Ressourcen sind der DNS-Name und die angehängten EIPs unterschiedliche Netzwerkeintrittspunkte, sodass Netzwerk-Scans für jeden von ihnen separate Ergebnisse liefern.

Beweise scannen

Wenn das Netzwerk-Scannen feststellt, dass ein Port erreichbar ist, umfasst das Ergebnis auch Hinweise auf den erreichbaren Dienst. Die folgenden Arten von Nachweisen können gesammelt werden:

TCP-Banner

Erste Byte, die vom Dienst bei der Verbindung gesendet werden, z. B. eine SSH-Versionszeichenfolge.

HTTP-Metadaten

Antwort-Header und HTTP-Statuscode.

TLS-Zertifikat

Allgemeiner Name (CN), Aussteller, Ablaufdatum und selbstsignierter Status.

Erkennung von Diensten

Identifizierte Anwendung oder Protokoll, das auf dem Port ausgeführt wird.

Ressourcen vom Scannen ausschließen

Um eine Ressource vom Netzwerkscannen auszuschließen, fügen Sie der Ressource den Tag-Schlüssel `SecurityHubNetworkScanExclusion` hinzu. Der Tag-Wert kann ein beliebiger Wert sein oder leer sein.

Sie müssen das Tag auf die tatsächliche Ressource mit der scannbaren öffentlichen IP anwenden:

- Für eine EIP, die an eine EC2-Instance angehängt ist, taggen Sie die EIP, nicht die EC2-Instance.
- Für eine EC2-Instance mit nur einer öffentlichen IP (ohne EIP) — kennzeichnen Sie die EC2-Instance.
- Bei einem Load Balancer — taggen Sie den Load Balancer und alle Ziele mit individuellen öffentlichen IP-Adressen.

Wenn Sie das Ausschluss-Tag hinzufügen, stoppt Network Scanning zukünftige Scans und schließt aktive Ergebnisse für diese Ressource. Wenn Sie das Tag entfernen, kann die Ressource erneut gescannt werden.

Unterstützte Anschlüsse

Network Scanning scannt die folgenden bekannten TCP-Ports auf geeigneten Ressourcen.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

Multi-cloud Unterstützung

Network Scanning unterstützt öffentliche Azure-IP-Adressen. Um Azure-Ressourcen zu scannen, erstellen Sie einen Security Hub-Connector für Ihre Azure-Umgebung. Weitere Informationen zur Integration mit Microsoft Azure finden Sie unter Integrieren von Security Hub mit Microsoft Azure.

Das Scanverhalten, die Nachweise und die Ergebnisse für Azure-Ressourcen sind identisch mit AWS Ressourcen. Die Ergebnisse werden zusammen mit den AWS Ergebnissen mit den entsprechenden Metadaten zum Cloud-Anbieter und zur Region angezeigt.

Verfügbarkeit in Regionen

Network Scanning ist in kommerziellen AWS Regionen verfügbar, in denen Security Hub verfügbar ist.

Deaktivieren Sie das Scannen im Netzwerk

Wenn Ihre Organisation Konfigurationsrichtlinien verwendet, kann der delegierte Administrator das Netzwerkscannen für bestimmte Konten und Regionen deaktivieren, indem er die Konfigurationsrichtlinie bearbeitet. Weitere Informationen zum Bearbeiten einer Konfigurationsrichtlinie finden Sie unter Bearbeiten einer Konfigurationsrichtlinie. Wählen Sie bei der Bearbeitung der Richtlinie die Funktion Netzwerkscanning aus, wählen Sie Deaktivieren und geben Sie dann die Konten und Regionen an, in denen Sie das Scannen deaktivieren möchten.

Für Konten, die nicht durch eine Konfigurationsrichtlinie verwaltet werden, können Sie den Netzwerk-Scan mit einer der folgenden Methoden deaktivieren.

Security Hub console

Um den Netzwerk-Scan zu deaktivieren

1. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Allgemeine Einstellungen aus.
3. Suchen Sie den Abschnitt Netzwerk-Scannen.
4. Wählen Sie Disable (deaktivieren) aus.
5. Bestätigen Sie, dass Sie den Netzwerk-Scan deaktivieren möchten.

Security Hub API

Rufen Sie die `DisableSecurityHubFeatureV2` API mit dem Funktionsnamen `NETWORK_SCANNING` auf.

AWS CLI

Führen Sie den folgenden Befehl aus, um das Netzwerkscannen zu deaktivieren:

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Wenn Sie den Netzwerk-Scan deaktivieren:

- Das Scannen im Netzwerk löst keine neuen Scans aus.
- Bestehende Ergebnisse bleiben sichtbar, bis sie im normalen Security Hub-Suchzyklus gelöscht werden.
- Der Netzwerk-Scan schließt alle bereits laufenden Scans ab.

Behebungspläne in Security Hub

Ein Abhilfeplan in AWS Security Hub gruppiert verwandte Risikofeststellungen, die eine gemeinsame Ursache haben. Jeder Plan zielt auf eine einzelne Ressource in Ihrer AWS Umgebung ab. Wenn Sie diese Ressource reparieren, können Sie den Schweregrad mehrerer Risiken gleichzeitig beheben oder verringern.

Ähnliche Risiken sind häufig auf dasselbe grundlegende Problem zurückzuführen, z. B. auf eine Fehlkonfiguration oder eine zu freizügige Einstellung für eine Ressource. Anstatt für jedes Risiko eine separate Maßnahme aufzulisten, gruppiert ein Abhilfeplan diese Risiken nach ihrer gemeinsamen Ursache. Sie gehen die Ursache einmal an und reduzieren das größte Risiko mit den wenigsten Maßnahmen.

Weitere Informationen zu Expositionsergebnissen finden Sie unterErkenntnisse zu Sicherheitsrisiken in Security Hub.

So erstellt Security Hub Behebungspläne

Security Hub erstellt anhand der in Ihrem Konto festgestellten Gefahren Abhilfemaßnahmen. Es generiert einen Plan für jede Kombination aus Zielressource und Risikomerkmal, gegen die es vorgehen kann.

Security Hub priorisiert Ihre Pläne, sodass diejenigen, die das größte Risiko reduzieren, zuerst angezeigt werden. Die Priorität hilft Ihnen bei der Entscheidung, woran Sie zuerst arbeiten möchten.

Wenn Security Hub ein neues Sicherheitsrisiko erkennt, wird möglicherweise nicht sofort ein Plan dafür angezeigt.

Einzelheiten zum Abhilfeplan

Jeder Behebungsplan enthält die folgenden Details.

- Priorität — Wie dringend Sie den Plan umsetzen sollten. Der Wert ist Kritisch, Hoch, Mittel oder Niedrig.
- Status — Der aktuelle Status des Plans. Der Wert ist „Neu“, „Aktualisiert“ oder „Gelöst“. Informationen zur Bedeutung der einzelnen Status finden Sie unterStatus des Sanierungsplans.
- Auswirkung — Wie der Plan Ihre Risiken verändert. Mit einem Plan können einige Risiken vollständig behoben, der Schweregrad anderer Risiken verringert und andere Risiken behoben werden, ohne deren Schweregrad zu ändern. Der Wert gibt in jedem Fall die Anzahl an.
- Rollout — Gibt an, ob der Fix sofort angewendet wird oder eine Bereitstellung erfordert. Der Wert lautet „Sofort“ oder „Bereitstellung erforderlich“.
- Aktion — Die Änderung, die der Plan empfiehlt.
- Merkmal — Das Expositionsmerkmal, auf das sich der Plan bezieht.
- Zielressource — Die Ressource, die im Plan festgelegt ist, und ihr Ressourcentyp.

- Konto und Region — AWS-Konto Derjenige, dem die Zielressource gehört, und ihre AWS-Region.

In einem Plan werden auch der betroffene Umfang, das Risikoniveau, die Umkehrbarkeit und der Automatisierungsgrad angegeben und angegeben, ob eine Überprüfung durch einen Mitarbeiter erforderlich ist, sofern dies in den Leitlinien vorgesehen ist.

Status des Sanierungsplans

Security Hub legt den Status jedes Plans fest. Sie können ihn nicht direkt ändern.

Neu

Security Hub hat den Plan erstellt, und der Plan hat sich seitdem nicht geändert.

Aktualisiert

Der Plan wurde geändert, nachdem Security Hub ihn erstellt hatte. So haben sich beispielsweise die Priorität, die Auswirkungen, die betroffenen Risiken oder die Leitlinien geändert. Der Plan behält diesen Status bei, bis er gelöst ist.

Gelöst

Der Plan muss nicht mehr angewendet werden. Security Hub löst einen Plan auf, wenn er den Plan nicht mehr anhand Ihrer aktuellen Risiken generiert. Dies ist der Fall, wenn die Risiken des Plans behoben, unterdrückt oder archiviert werden, wenn ihr Schweregrad auf Informativ geändert wird oder wenn sie nicht mehr das Merkmal aufweisen, auf das sich der Plan bezieht.

Ein aufgelöster Plan bedeutet nicht immer, dass seine Risikofeststellungen behoben sind. Beispielsweise besteht eine Exposition, deren Schweregrad sich auf Informativ ändert, immer noch.

Ein gelöster Plan bleibt etwa 14 Tage in der Liste, danach entfernt Security Hub ihn. Wenn der Plan erneut angewendet werden muss, ändert sich sein Status in Neu.

Anleitung zur Problembehebung

Jeder Behebungsplan enthält Anleitungen, in denen beschrieben wird, wie das Problem behoben werden kann. Sie öffnen einen Plan, um die zugehörigen Anleitungen im Abschnitt Anleitungen auf der Registerkarte „Übersicht“ zu lesen.

> **Note**
>
> Security Hub beschreibt die Schritte, und Sie wenden sie selbst an. Security Hub ändert Ihre Ressourcen nicht für Sie.

In der Anleitung sind die Schritte in Phasen unterteilt, z. B. Voraussetzung, Snapshot, Korrektur, Verifizierung und Fertig. Die einzelnen Phasen und ihr Inhalt stammen aus den Anleitungen für die Zielressource.

Ein Schritt kann auch einen Rollback beinhalten, der beschreibt, wie dieser Schritt rückgängig gemacht werden kann.

Anleitungen können Beispielbefehle in mehr als einem Format enthalten, z. B. AWS CLI Azure CLI, Python, Terraform, CDK CloudFormation, Bicep und ARM-Vorlage. Die verfügbaren Formate stammen aus den Anleitungen für die Zielressource. Wenn für die Zielressource keine Leitlinien verfügbar sind, wird im Abschnitt stattdessen darüber berichtet.

Behebungspläne anzeigen

Sie können Ihre Behebungspläne auf der Seite Behebungspläne in der Security Hub Hub-Konsole einsehen.

Um Behebungspläne einzusehen

1. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Reaktion die Option Remediations aus.

Auf der Seite „Behebungspläne“ werden Ihre Behebungspläne in einer Tabelle aufgeführt. In jeder Zeile werden die empfohlene Maßnahme, die Priorität des Plans, die Zielressource mit ihrem AWS-Region und sowie die Auswirkungen AWS-Konto, der Status und die Einführung des Plans angezeigt. Was diese bedeuten, finden Sie unterEinzelheiten zum Abhilfeplan.

Sie können die Liste nicht nach Spalten sortieren.

Behebungspläne filtern

Verwenden Sie die Leiste Behebungspläne filtern, um die Liste einzugrenzen. Sie können nach den folgenden Eigenschaften filtern:

- Priorität
- Status
- Ressourcentyp
- Cloud-Anbieter
- Zielressourcen-ID
- Account

Für diese Filter gelten die folgenden Grenzwerte:

- Jeder Filter entspricht Werten nur nach Gleichheit. Sie können keine teilweisen Übereinstimmungen oder Bereiche verwenden.
- Sie können bis zu zwei Filter gleichzeitig anwenden. Security Hub kombiniert sie mit`AND`, sodass ein Plan beiden Filtern entsprechen muss, damit er angezeigt wird.
- Bei Werten wird zwischen Groß- und Kleinschreibung unterschieden. Geben Sie als Ressourcentyp den vollständigen Typ ein, wie er in der Liste angezeigt wird, z. `AWS::EC2::Instance` B.

Die Risiken anzeigen, auf die sich ein Plan auswirkt

Wenn Sie einen Behebungsplan öffnen, enthält der Detailbereich die Registerkarte Betroffene Risiken. Auf dieser Registerkarte werden die Ergebnisse der Risiken aufgeführt, auf die sich der Plan bezieht. Für jedes Risiko werden der Titel des Risikos, die Art und Weise, wie der Plan ihn ändert, und die daraus resultierende Änderung des Schweregrads angezeigt.

Ein Risiko, das im Plan berücksichtigt wird, ohne den Schweregrad zu verringern, weist statt einer Änderung nur einen Schweregradwert auf.

Wenn ein Plan mehr Risiken betrifft, als auf der Registerkarte angezeigt werden, wird auf der Registerkarte angezeigt, wie viele Risiken angezeigt werden.

Abhilfepläne für ein Risiko anzeigen

Wenn Sie sich ein Risikoergebnis ansehen, enthält das Detailfenster die Registerkarte Abhilfemaßnahmen. Auf dieser Registerkarte sind die Behebungspläne aufgeführt, die sich mit dem Risiko befassen. Ein Risiko kann mehr als einen Plan haben.

Jeder Plan zeigt die empfohlene Maßnahme, ihre Priorität und die Zielressource mit ihrem Ressourcentyp. Erweitern Sie einen Plan, um die zugehörigen Leitlinien zu lesen.

Nachverfolgung der Auswirkungen von Abhilfemaßnahmen auf dem Dashboard

Das Übersichts-Dashboard enthält ein Widget für Behebungspläne. Das Widget listet bis zu fünf Pläne mit dem Status Neu oder Aktualisiert auf, sortiert nach Priorität, sodass Sie die dringendsten Aufgaben bearbeiten können, ohne die vollständige Liste öffnen zu müssen.

Für jeden Plan zeigt das Widget die empfohlene Maßnahme, die Priorität des Plans, seine Auswirkungen, die Zielressource und die Person, der AWS-Konto die Ressource gehört, an. Um zu sehen, welche Risiken hinter einem Plan stehen, wählen Sie dessen Wirkung aus.

Das Widget berichtet über die Auswirkungen der einzelnen Pläne. Es kombiniert die Auswirkungen der einzelnen Pläne nicht, sodass jedes Risiko, das von mehr als einem Plan abgedeckt wird, in jedem dieser Pläne berücksichtigt wird.

Sie können keine Filter auf dieses Widget anwenden.

Automatisierungen im Security Hub

Security Hub umfasst Funktionen, die Ergebnisse automatisch ändern und auf der Grundlage Ihrer Spezifikationen Maßnahmen ergreifen.

Security Hub unterstützt derzeit die folgenden Arten von Automatisierungen:

- Automatisierungsregeln — Automatisches Aktualisieren und Unterdrücken von Ergebnissen sowie Senden der Ergebnisse an Ticketing-Tools — nahezu in Echtzeit auf der Grundlage definierter Kriterien.
- Automatisierte Reaktion und Problembehebung — Erstellen Sie benutzerdefinierte EventBridge Amazon-Regeln, die automatische Maßnahmen definieren, die anhand bestimmter Ergebnisse und Erkenntnisse ergriffen werden.

Automatisierungsregeln sind hilfreich, wenn Sie Suchfelder im Open Cybersecurity Schema Framework (OCSF) automatisch aktualisieren möchten. Sie können beispielsweise eine Automatisierungsregel verwenden, um den Schweregrad der Ergebnisse für Ressourcen mit einem bestimmten Tag zu aktualisieren. Durch die Verwendung der Automatisierungsregel entfällt die Notwendigkeit, den Schweregrad jedes Befundes, das sich auf ein bestimmtes Tag bezieht, manuell zu aktualisieren. Sie können Automatisierungsregeln so konfigurieren, dass Tickets in Tools wie Jira Cloud und ServiceNow wenn Ergebnisse bestimmten Attributen entsprechen, erstellt werden. Tickets werden anhand der Ergebnisse erstellt, sobald sie in Security Hub eintreffen.

EventBridge Regeln sind hilfreich, wenn Sie für bestimmte Ergebnisse außerhalb von Security Hub Maßnahmen ergreifen oder bestimmte Ergebnisse zur Behebung oder weiteren Untersuchung an Tools von Drittanbietern senden möchten. Die Regeln können verwendet werden, um unterstützte Aktionen auszulösen, z. B. das Aufrufen einer AWS Lambda Funktion oder das Informieren eines Amazon Simple Notification Service (Amazon SNS) -Themas über ein bestimmtes Ergebnis.

Automatisierungsregeln werden wirksam, bevor EventBridge Regeln angewendet werden. Das heißt, Automatisierungsregeln werden ausgelöst und aktualisieren ein Ergebnis, bevor das EventBridge Ergebnis eingeht. EventBridge Die Regeln gelten dann für das aktualisierte Ergebnis.

Automatisierungsregeln in Security Hub

Mit Security Hub können Sie Aufgaben wie das Aktualisieren von Funddetails, das Aktualisieren der Wichtigkeit Ihrer Ressourcen und das Erstellen von Tickets für Integrationen von Drittanbietern automatisieren.

Automatisierungsregeln und AWS-Regionen

Automatisierungsregeln können in einem erstellt AWS-Region und dann in allen konfigurierten Regeln angewendet werden AWS-Regionen. Wenn Sie die Regionsaggregation verwenden, können Sie Regeln nur in der Heimatregion erstellen. Wenn Sie Regeln in der Heimatregion erstellen, wird jede Regel, die Sie definieren, auf alle verknüpften Regionen angewendet, es sei denn, Ihre Regelkriterien schließen eine bestimmte verknüpfte Region aus. Sie müssen eine Automatisierungsregel für jede Region erstellen, die keine verknüpfte Region ist.

Arten von Automatisierungsregeln

Automatisierungsregeln in Security Hub unterstützen zwei Regeltypen: Suchregeln und Ressourcenregeln. Eine Suchregel gleicht Ergebnisse ab und aktualisiert die Funddetails oder erstellt ein Ticket für eine Drittanbieter-Integration. Eine Ressourcenregel ordnet Ressourcen zu und legt die Wichtigkeit dieser Ressourcen fest. Eine einzelne Regel verwendet entweder Suchkriterien oder

Ressourcenkriterien, aber nicht beide. Eine Ressourcenregel verknüpft Ressourcenkriterien mit der Ressourcenaktion, um die Priorität festzulegen, und sie kann keine Ergebnisdetails aktualisieren oder ein Ticket erstellen.

Suchregeln und Ressourcenregeln haben dasselbe Kontingent. Sie können jeweils maximal 100 Automatisierungsregeln pro Konto erstellen AWS-Region, sowohl für Such- als auch für Ressourcenregeln.

Nach Regelaktionen und Kriterien suchen

Automatisierungsregeln in Security Hub verwenden Kriterien, um in Security Hub Hub-Ergebnissen auf OCSF-Attribute zu verweisen. Beispielsweise stimmen die für den `Criteria` Parameter in unterstützten Filter mit den Filtern CreateAutomationRuleV2überein, die für den `Filters` Parameter in GetFindingsV2 unterstützt werden. Das bedeutet, dass Filter, die in Automatisierungsregeln verwendet werden, verwendet werden können, um Ergebnisse zu erhalten. Security Hub unterstützt die folgenden OCSF-Felder für Automatisierungsregelkriterien.

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
`activity_id`	`Activity ID`	`Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)`	`Number`
`activity_name`	`Provider status`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`
`class_name`	`Finding class name`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
cloud.account.name	Finding account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.account.uid	Account ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.region	Region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.category	Assessment category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
compliance.assessments.name	Assessment name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control	Security control ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control_parameters	Control parameter name	EQUALS	Map
compliance.standards	Applicable standards	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status	Compliance status	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.created_time_dt	Created at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.desc	Finding description	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.first_seen_time_dt	First observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.last_seen_time_dt	Last observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
finding_info.related_events.product.uid	Related findings product ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.title	Related findings title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.traits.category	Traits category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.uid	Related findings ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
finding_info.src_url	Source URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.tags	Finding info tags	EQUALS	Map
finding_info.title	Finding title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.types	Finding type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider finding ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
metadata.product.name	Product name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.uid	Product ARN	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.references	Recommendation URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
resources.cloud_partition	Resource partition	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.modified_time_dt	Resource last modified time	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
resources.name	Resource name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.name	Account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.uid	Account	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.org.uid	Organization	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
resources.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.region	Resource region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.tags	Resource tags	EQUALS	Map
resources.type	Resource type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.uid	Resource ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vendor_attributes.severity	Provider severity	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
vendor_attributes.severity_id	Provider severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.affected_code.file.path	Affected code file path	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.affected_packages.name	Affected package name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.cvss.base_score	CVE CVSS base score	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.cve.epss.score	Epss score	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF-Feld	Wert des Konsolenfilters	Filteroperatoren	Feldtyp
vulnerabilities.cve.uid	Vulnerability ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.fix_coverage	Software vulnerabilities coverage	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
vulnerabilities.related_vulnerabilities	Related vulnerabilities	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bei Kriterien, die als Zeichenkettenfelder gekennzeichnet sind, wirkt sich die Verwendung verschiedener Filteroperatoren für dasselbe Feld auf die Bewertungslogik aus. Weitere Informationen finden Sie StringFilterin der Security Hub Hub-API-Referenz.

Jedes Kriterium unterstützt eine maximale Anzahl von Werten, anhand derer übereinstimmende Ergebnisse gefiltert werden können. Die Grenzen der einzelnen Kriterien finden Sie OcsfFindingFiltersin der Security Hub Hub-API-Referenz

OCSF-Felder, die aktualisiert werden können

Im Folgenden sind die OCSF-Felder aufgeführt, die mithilfe von Automatisierungsregeln aktualisiert werden können.

- `Comment`
- `SeverityId`
- `StatusId`

Aktionen und Kriterien für Ressourcenregeln

Ressourcenkriterien verweisen auf Ressourcenattribute. Die für Ressourcenkriterien unterstützten Filter sind eine Teilmenge der Filter, die für den GetResourcesV2-Vorgang unterstützt werden. Sie können Filter mit `OR` Operatoren `AND` und kombinieren und sie bis zu drei Ebenen mit maximal 100 Filtern pro Regel verschachteln.

Security Hub unterstützt die folgenden Ressourcenfelder für Ressourcenkriterien.

Feld „Ressource“	Wert für den Konsolenfilter	Filteroperatoren	Feldtyp
`ResourceId`	`Resource ID`	`EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`
`ResourceName`	`Resource name`	`EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`

Feld „Ressource“	Wert für den Konsolenfilter	Filteroperatoren	Feldtyp
ResourceType	Resource type	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceCategory	Resource category	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceSubCategory	Resource sub-category	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceProvider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceCloudPartition	Resource partition	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Feld „Ressource“	Wert für den Konsolenfilter	Filteroperatoren	Feldtyp
ResourceRegion	Region	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceGuid	Resource GUID	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AccountId	Finding account	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AccountName	Account name	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Region	Finding region	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Feld „Ressource“	Wert für den Konsolenfilter	Filteroperatoren	Feldtyp
ResourceOwnerAccountId	Account	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceOwnerOrgId	Organization	EQUALS, PREFIX, CONTAINS, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceCreationTime	Created at	Start, End, DateRange	Date
ResourceDetailCaptureTime	Resource detail capture time	Start, End, DateRange	Date
ResourceTags	Resource tags	EQUALS, NOT_EQUALS, CONTAINS, NOT_CONTAINS	Map

Security Hub unterstützt keine Zahlenfilter. Der `CONTAINS_WORD` Operator für Ressourcenkriterien wird nicht unterstützt. Die vollständige Liste der Ressourcenfilterfelder und ihrer zulässigen Werte finden Sie unter ResourcesFiltersund GetResourcesV2 in der Security Hub API-Referenz.

Ressourcenfelder, die aktualisiert werden können

Eine Ressourcenregel aktualisiert die Wichtigkeit von Ressourcen, die Ihren Kriterien entsprechen. Sie können die Priorität auf einen der folgenden Werte festlegen, die vom höchsten zum niedrigsten Wert aufgelistet sind.

- `Very High`
- `High`
- `Medium`
- `Low`
- `Unknown`

Ressourcenregeln gelten nicht für selbst gehostete KI-Ressourcen. Diese Ressourcentypen sind von der Priorität der Automatisierungsregeln ausgenommen, und sie erhalten weiterhin eine abgeleitete Priorität.

Wie Automatisierungsregeln die Ergebnisse bewerten

Eine Automatisierungsregel wertet neue und aktualisierte Ergebnisse aus, die Security Hub generiert oder aufnimmt, nachdem Sie die Regel erstellt haben.

Automatisierungsregeln bewerten ursprüngliche, vom Anbieter bereitgestellte Ergebnisse. Durch die Integration mit Security Hub können Anbieter neue Erkenntnisse liefern und bestehende Erkenntnisse aktualisieren. Regeln werden nicht ausgelöst, wenn Sie Suchfelder nach der Regelerstellung im Rahmen des `BatchUpdateFindingsV2` Vorgangs aktualisieren. Wenn Sie eine Automatisierungsregel erstellen und eine `BatchUpdateFindingsV2` Aktualisierung vornehmen, die sich beide auf dasselbe Ergebnisfeld auswirken, legt die letzte Aktualisierung den Wert für dieses Feld fest. Nehmen wir das folgende Beispiel:

Sie verwenden`BatchUpdateFindingsV2`, um das `Status` Feld eines Befundes von bis `New` zu zu aktualisieren`In Process`. Wenn Sie aufrufen`GetFindingsV2`, hat das `Status` Feld jetzt den Wert`In Process`. Sie erstellen eine Automatisierungsregel, die das `Status` Feld des Ergebnisses von `New` zu ändert `Suppressed` (denken Sie daran, dass Regeln Aktualisierungen ignorieren, die mit vorgenommen wurden`BatchUpdateFindingsV2`). Der Suchprovider aktualisiert den Befund und ändert das `Status` Feld in`New`. Wenn Sie aufrufen`GetFindingsV2`, hat das `Status` Feld jetzt den Wert, `Suppressed` weil die Automatisierungsregel angewendet wurde und die Regel die letzte Aktion war, die auf das Ergebnis angewendet wurde.

Wenn Sie eine Regel auf der Security Hub Hub-Konsole erstellen oder bearbeiten, zeigt die Konsole eine Vorschau der Ergebnisse an, die den Regelkriterien entsprechen. Während Automatisierungsregeln die ursprünglichen Ergebnisse auswerten, die vom Anbieter der Ergebnisse gesendet wurden, werden in der Konsolenvorschau die Ergebnisse in ihrem endgültigen Zustand

wiedergegeben, so wie sie als Reaktion auf den `GetFindingsV2` API-Vorgang angezeigt würden (d. h. nachdem Regelaktionen oder andere Aktualisierungen auf das Ergebnis angewendet wurden).

Wie sind die Automatisierungsregeln angeordnet

Jeder Automatisierungsregel wird eine Regelreihenfolge zugewiesen. Dies bestimmt die Reihenfolge, in der Security Hub Ihre Automatisierungsregeln anwendet, und ist wichtig, wenn sich mehrere Regeln auf dasselbe Ergebnis oder Findungsfeld beziehen.

Wenn sich mehrere Regelaktionen auf dasselbe Befund- oder Findungsfeld beziehen, gilt die Regel mit dem höchsten numerischen Wert für die Reihenfolge der Regeln zuletzt und hat die endgültige Wirkung.

Die Reihenfolge der Regeln bestimmt auch die endgültige Kritikalität einer Ressource. Wenn mehrere Ressourcenregeln derselben Ressource entsprechen, bestimmt die Regel, die zuletzt gilt, die Priorität der Ressource.

Wenn Sie eine Regel in der Security Hub-Konsole erstellen, weist Security Hub automatisch die Regelreihenfolge auf der Grundlage der Reihenfolge der Regelerstellung zu. Die erste Regel, die Sie erstellen, hat die Regelreihenfolge 1. Wenn mehr als eine Regel vorhanden ist, hat jede anschließend erstellte Regel den nächsthöheren verfügbaren numerischen Wert für die Regelreihenfolge.

Wenn Sie eine Regel über CreateAutomationRuleV2API oder erstellen AWS CLI, wendet Security Hub `RuleOrder` zuerst die Regel mit dem niedrigsten numerischen Wert an. Anschließend werden nachfolgende Regeln in aufsteigender Reihenfolge angewendet. Wenn mehrere Ergebnisse identisch sind`RuleOrder`, wendet Security Hub zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die Regel, die zuletzt bearbeitet wurde, gilt zuletzt).

Sie können die Reihenfolge der Regeln jederzeit ändern.

Beispiel für die Reihenfolge der Regeln:

Regel A (Regelreihenfolge ist**1**):

- Kriterien für Regel A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` ist `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` ist `NEW`
  - `Workflow.Status` = `ACTIVE`

- Aktionen nach Regel A
  - Update `Confidence` auf `95`
  - Aktualisieren `Severity` auf `CRITICAL`
  - Aktualisieren `Comment` auf `This needs attention`

Regel B (Reihenfolge der Regeln ist**2**):

- Kriterien für Regel B
  - `AwsAccountId` = `123456789012`
- Aktionen nach Regel B
  - Update `Severity` auf `INFORMATIONAL`

Erstens gelten die Aktionen nach Regel A für Security Hub Hub-Ergebnisse, die den Kriterien von Regel A entsprechen. Anschließend gelten die Aktionen nach Regel B für Security Hub Hub-Ergebnisse mit der angegebenen Konto-ID. Da Regel B in diesem Beispiel zuletzt gilt, lautet der Endwert von `Severity` in findings from the specified account ID`INFORMATIONAL`. Basierend auf der Regel A-Aktion ist der Endwert von `Confidence` in übereinstimmenden Ergebnissen`95`.

Third-party Integrationen

Sie können Automatisierungsregeln verwenden, um Tickets für Integrationen mit Jira Cloud und zu erstellen. ServiceNow ITSM Weitere Informationen finden Sie unter Regel für eine Drittanbieter-Integration erstellen.

Szenarien, in denen Automatisierungsregeln nicht funktionieren

Im Folgenden sind Szenarien aufgeführt, in denen Automatisierungsregeln nicht funktionieren.

- Das eigenständige Konto wird Mitglied einer Organisation mit einem delegierten Administrator
- Das Organisationsverwaltungskonto entfernt den delegierten Administrator und richtet einen neuen delegierten Administrator ein
- Die Aggregatorkonfiguration für den delegierten Administrator oder das eigenständige Konto ändert sich, wenn aus einer Region ohne Verknüpfung eine verknüpfte Region wird

In diesen Szenarien kann ein Mitglied einer Organisation Automatisierungsregeln mit Listen-, Abruf- und Löschvorgängen in den AWS CLI APIs oder verwalten.

Wenn eine nicht verknüpfte Region zu einer verknüpften Region gemacht wird, kann der delegierte Administrator oder das eigenständige Konto Ressourcen in einer verknüpften Region mit Auflisten-, Abruf- und Löschvorgängen verwalten.

Automatisierungsregeln in Security Hub erstellen

In diesem Thema wird beschrieben, wie Automatisierungsregeln erstellt werden. Sie können Automatisierungsregeln verwenden, um Details zu einem Ergebnis zu aktualisieren, die Wichtigkeit Ihrer Ressourcen zu aktualisieren oder ein Ticket für eine Drittanbieter-Integration zu erstellen. Sie müssen Automatisierungsregeln individuell und dort erstellen AWS-Region , wo sie angewendet werden sollen. Wenn Sie jedoch eine Automatisierungsregel in einer Aggregationsregion erstellen, wird sie in allen Regionen angewendet. Andernfalls, wenn Sie eine Automatisierungsregel in einer Region ohne Verknüpfung erstellen, wird sie nur in dieser Region angewendet.

Eine Regel erstellen, die die Suchdetails aktualisiert

Im folgenden Verfahren wird beschrieben, wie Sie eine Regel erstellen, die Funddetails aktualisiert.

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automations aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie unter Details einen Namen für Ihre Automatisierungsregel ein.
   - (Optional) Geben Sie eine Beschreibung für Ihre Automatisierungsregel ein.
5. Wählen Sie unter Aktionen die Option Ergebnisdetails aktualisieren aus. Sie können nach Kriterien suchen und Kriterien in der Suchleiste hinzufügen. Um zu überprüfen, ob Ergebnisse Ihren Kriterien entsprechen, wählen Sie Vorschau der passenden Ergebnisse aus.
6. Wählen Sie unter Ergebnisdetails aktualisieren mindestens ein Ergebnisdetail aus, das aktualisiert werden soll, wenn ein Ergebnis Ihren Kriterien entspricht. Sie können Schweregrad, Status oder Kommentar wählen.
7. Wählen Sie unter Regeleinstellungen die Option Aktiviert oder Deaktiviert aus. Wenn Sie Aktiviert auswählen, ist die Automatisierungsregel aktiviert und verarbeitet neue Ergebnisse. Wenn Sie Deaktiviert auswählen, ist die Automatisierungsregel deaktiviert und verarbeitet keine Ergebnisse.
8. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um ein Schlüssel-Wert-Paar einzugeben, das auf Ihre Automatisierungsregel angewendet werden soll.

9. Wählen Sie Regel erstellen aus.

Eine Regel erstellen, die die Ressourcenpriorität aktualisiert

Im folgenden Verfahren wird beschrieben, wie Sie eine Regel erstellen, die die Priorität von Ressourcen aktualisiert, die Ihren Kriterien entsprechen.

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automations aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie unter Details einen Namen für Ihre Automatisierungsregel ein.
   - (Optional) Geben Sie eine Beschreibung für Ihre Automatisierungsregel ein.
5. Wählen Sie unter Aktionen die Option Ressourcendetails aktualisieren aus. Sie können nach Kriterien suchen und Kriterien in der Suchleiste hinzufügen. Um zu überprüfen, ob Ressourcen Ihren Kriterien entsprechen, wählen Sie Vorschau der passenden Ressourcen aus.
6. Wählen Sie unter Ressourcendetails aktualisieren für Priorität die Priorität aus, die auf Ressourcen angewendet werden soll, die Ihren Kriterien entsprechen. Sie können „Sehr hoch“, „Hoch“, „Mittel“, „Niedrig“ oder „Unbekannt“ wählen.

   > **Note**
   >
   > Diese Regel gilt nicht für selbst gehostete KI-Ressourcen. Diese Ressourcentypen sind von der Priorität der Automatisierungsregeln ausgenommen.

7. Wählen Sie unter Regeleinstellungen die Option Aktiviert oder Deaktiviert aus. Wenn Sie Aktiviert auswählen, ist die Automatisierungsregel aktiviert und verarbeitet Ressourcen, die Ihren Kriterien entsprechen. Wenn Sie Deaktiviert auswählen, ist die Automatisierungsregel deaktiviert und verarbeitet keine Ressourcen.
8. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um ein Schlüssel-Wert-Paar einzugeben, das auf Ihre Automatisierungsregel angewendet werden soll.
9. Wählen Sie Regel erstellen aus.

Eine Regel für eine Drittanbieter-Integration erstellen

Im folgenden Verfahren wird beschrieben, wie Sie eine Regel erstellen, die ein Ticket für eine Drittanbieterintegration erstellt. Informationen zu den Integrationen, die Security Hub CSPM unterstützt, finden Sie unter Third-party Integrationen für Security Hub CSPM.

1. Loggen Sie sich in Ihr Konto ein. AWS Öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automations aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie unter Details einen Namen für Ihre Automatisierungsregel ein.
   - (Optional) Geben Sie eine Beschreibung für Ihre Automatisierungsregel ein.
5. Wählen Sie unter Aktionen die Option Ticket erstellen aus. Sie können nach Kriterien suchen und Kriterien in der Suchleiste hinzufügen. Um zu überprüfen, ob Ergebnisse Ihren Kriterien entsprechen, wählen Sie Vorschau der passenden Ergebnisse aus.
6. Wählen Sie unter Ticket erstellen eine IT-Ticketing-Integration aus der Dropdownliste aus und wählen Sie dann Integration hinzufügen aus.
7. Wählen Sie unter Regeleinstellungen die Option Aktiviert oder Deaktiviert aus. Wenn Sie Aktiviert auswählen, ist die Automatisierungsregel aktiviert und verarbeitet neue Ergebnisse. Wenn Sie Deaktiviert auswählen, ist die Automatisierungsregel deaktiviert und verarbeitet keine Ergebnisse.
8. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um ein Schlüssel-Wert-Paar einzugeben, das auf Ihre Automatisierungsregel angewendet werden soll.
9. Wählen Sie Regel erstellen aus.

Details für Automatisierungsregeln in Security Hub anzeigen

In diesem Thema wird beschrieben, wie Details für Automatisierungsregeln angezeigt werden. Sie können die folgenden Details für eine Automatisierungsregel anzeigen:

- Name und Beschreibung
- Aktionen und Kriterien
- Status der Regel und bestehende Ergebnisse
- Tags (Markierungen)

Um Details für eine Automatisierungsregel anzuzeigen

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automatisierungen aus. Auf diesem Bildschirm werden alle von Ihnen erstellten Automatisierungsregeln angezeigt.
3. Wählen Sie die Automatisierungsregel aus, die Sie anzeigen möchten. Wählen Sie die Option Details anzeigen aus. Alternativ können Sie den Namen der Automatisierungsregel wählen, die Sie anzeigen möchten.

Aktualisierung der Regelreihenfolge in Security Hub

In diesem Thema wird beschrieben, wie die Regelreihenfolge für Automatisierungsregeln in der Konsole aktualisiert wird. Wenn Sie die Kriterien für eine Automatisierungsregel bearbeiten möchten, finden Sie weitere Informationen unter Automatisierungsregeln in Security Hub bearbeiten.

Sie können die Regelreihenfolge für eine Automatisierungsregel nicht aktualisieren, ohne die Regelreihenfolge für jede Automatisierungsregel zu aktualisieren. Sie haben beispielsweise vier Automatisierungsregeln: Regel A (1), Regel B (2), Regel C (3) und Regel D (4). Sie möchten, dass Regel D zuerst angewendet wird. Dazu ändern Sie die Zahl von 4 auf 1. Als Ergebnis erhält Regel A 2, Regel B erhält 3 und Regel C erhält 4.

Um die Regelreihenfolge für Ihre Automatisierungsregeln zu aktualisieren

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie bearbeiten möchten. Wählen Sie unter Bestellung das Stiftsymbol neben der Bestellnummer aus. Verwenden Sie die Pfeile, um die neue Bestellnummer zu ermitteln. Wählen Sie zur Bestätigung das Symbol ✓. Wählen Sie das X-Symbol, um den Vorgang abzubrechen. Alternativ können Sie Reihenfolge ändern wählen, um die Automatisierungsregel in der Liste nach unten, oben oder an den Anfang zu verschieben.

Automatisierungsregeln in Security Hub deaktivieren

In diesem Thema wird beschrieben, wie Automatisierungsregeln deaktiviert werden. Wenn Sie Automatisierungsregeln deaktivieren, wendet Security Hub sie nicht mehr an. Sie können Automatisierungsregeln jederzeit und dort deaktivieren, AWS-Region wo Sie sie erstellt haben.

Um eine Regel zu deaktivieren

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie deaktivieren möchten. Wählen Sie unter Status das Stiftsymbol neben Aktiviert aus. Wählen Sie das Drop-down-Menü und dann Deaktiviert aus. Wählen Sie zur Bestätigung das Symbol ✓. Wählen Sie das X-Symbol, um den Vorgang abzubrechen. Sie können auch im Drop-down-Menü „Aktionen“ die Option „Deaktivieren“ auswählen.

Eine Automatisierungsregel in Security Hub aktivieren

In diesem Thema wird beschrieben, wie Automatisierungsregeln aktiviert werden. Wenn Sie Automatisierungsregeln aktivieren, wendet Security Hub sie wieder an. Sie können Automatisierungsregeln jederzeit und dort aktivieren, AWS-Region wo Sie sie erstellt haben.

Um eine Regel zu aktivieren

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie aktivieren möchten. Wählen Sie unter Status das Stiftsymbol neben Deaktiviert aus. Wählen Sie das Drop-down-Menü aus und wählen Sie dann Aktiviert aus. Wählen Sie zur Bestätigung das Symbol ✓. Wählen Sie das X-Symbol, um den Vorgang abzubrechen. Sie können auch im Drop-down-Menü „Aktionen“ die Option „Aktivieren“ auswählen.

Automatisierungsregeln in Security Hub duplizieren

In diesem Thema wird beschrieben, wie Automatisierungsregeln dupliziert werden. Das Duplizieren von Automatisierungsregeln kann Ihnen helfen, Zeit zu sparen, wenn Sie vermeiden möchten, sie von Grund auf neu zu erstellen. Wenn Sie Automatisierungsregeln duplizieren, können Sie Details, Aktionen, Regeleinstellungen und Tags aktualisieren. Sie können Automatisierungsregeln dort bearbeiten AWS-Region , wo Sie sie erstellt haben.

Um eine Regel zu duplizieren

1. Melden Sie sich bei Ihrem AWS Konto an und öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Verwaltung und dann Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie duplizieren möchten. Wählen Sie dann Aktionen und dann Duplizieren aus.
4. Nehmen Sie Ihre Änderungen vor, überprüfen Sie sie und wählen Sie dann Regel erstellen aus.

Automatisierungsregeln in Security Hub bearbeiten

In diesem Thema wird beschrieben, wie Automatisierungsregeln bearbeitet werden. Sie können Automatisierungsregeln dort bearbeiten AWS-Region , wo Sie sie erstellt haben.

Sie können Folgendes für Automatisierungsregeln bearbeiten:

- Name und Beschreibung
- Aktionen
- Regeleinstellungen

Sie können die Tags für Automatisierungsregeln nicht bearbeiten.

Um eine Regel zu bearbeiten

1. Loggen Sie sich in Ihr AWS Konto ein. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie bearbeiten möchten. Wählen Sie Actions und anschließend Bearbeiten.

4. Nehmen Sie Ihre Änderungen vor und überprüfen Sie sie.
5. Wählen Sie Änderungen speichern aus.

Löschen von Automatisierungsregeln in Security Hub

In diesem Thema wird beschrieben, wie Automatisierungsregeln gelöscht werden. Sie können Automatisierungsregeln dort löschen AWS-Region , wo Sie sie erstellt haben.

So löschen Sie eine Regel

1. Melden Sie sich bei Ihrem AWS Konto an und öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Verwaltung und dann Automatisierungen aus.
3. Wählen Sie die Automatisierungsregel aus, die Sie löschen möchten. Wählen Sie Actions und anschließend Delete.
4. Wählen Sie Delete (Löschen).

Automatisierungsregeln in EventBridge

Sie können Automatisierungsregeln in Amazon verwenden EventBridge , um auf Security Hub-Ergebnisse zu reagieren. Security Hub sendet Ergebnisse nahezu in Echtzeit EventBridge als Ereignisse an. Sie können grundlegende Regeln schreiben, die angeben, welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis einer Regel entspricht. Zu den Aktionen, die automatisch ausgelöst werden können, gehören:

- Konfiguration eines API-Ziels in EventBridge.
- Amazon EC2-Ausführungsbefehle aufrufen
- Aufrufen von Lambda-Funktionen
- Zustandsautomaten von Step Functions aufrufen
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange
- Ereignisse an Kinesis Data Streams weiterleiten
- Senden eines Funds an ein Ticketing-, Chat-, SIEM- oder Incident-Response- und Management-Tool eines Drittanbieters
- Ein Ereignis an einen EventBridge Bus in einem anderen Konto senden AWS

Security Hub sendet neue und aktualisierte Ergebnisse EventBridge als Ereignisse an. Anschließend konfigurieren Sie EventBridge Regeln, um auf jedes Security Hub-Ereignis zu reagieren. Weitere Informationen finden Sie unter Was ist EventBridge? im EventBridge Benutzerhandbuch.

> **Note**
>
> Wenn Sie in Security Hub CSPM EventBridge Regeln für Ergebnisse definiert haben, können sich die Regeln mit den für Security Hub definierten Regeln überschneiden. Um zu vermeiden, dass doppelte Ergebnisse gesendet werden, überprüfen Sie die Regeln, die Sie für Security Hub CSPM definiert haben, um festzustellen, ob sie sich mit den Regeln überschneiden, die Sie für Security Hub definiert haben. Deaktivieren Sie gegebenenfalls alle Security Hub CSPM-Regeln, die durch Security Hub-Regeln ersetzt wurden.

> **Note**
>
> Es hat sich bewährt, sicherzustellen, dass Benutzer mit Zugriffsberechtigungen AWS Identity and Access Management Richtlinien EventBridge verwenden, die die erforderlichen Mindestberechtigungen gewähren. Weitere Informationen finden Sie unter EventBridge und AWS Identity and Access Management im EventBridge Benutzerhandbuch.

EventBridge Ereignistypen

Security Hub verwendet die folgenden EventBridge Amazon-Ereignistypen für die Integration EventBridge.

Auf dem EventBridge Dashboard für Security Hub umfasst All Events all diese Ereignistypen.

Ergebnisse wurden importiert (V2)

Security Hub sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Findings Imported V2 Ereignisse. Jedes Findings Imported V2 Ereignis enthält ein einzelnes Ergebnis.

Jedes Ergebnis, das importiert wird, und jedes Ergebnis, das durch eine `BatchUpdateFindingsV2` Anfrage aktualisiert wird, löst ein Findings Imported V2 Ereignis aus.

Für Administratorkonten EventBridge enthält der Event-Feed Ereignisse für Ergebnisse sowohl aus ihrem Konto als auch aus ihren Mitgliedskonten.

In einer Aggregationsregion enthält der Event-Feed Ereignisse für Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Cross-Region Die Ergebnisse werden nahezu in Echtzeit in den Event-Feed aufgenommen.

Sie können Regeln definieren EventBridge , die Ergebnisse automatisch an einen Problembehebungsworkflow, ein Drittanbieter-Tool oder ein anderes unterstütztes EventBridge Ziel weiterleiten. Die Regeln können Filter enthalten, die die Regel nur anwenden, wenn das Ergebnis bestimmte Attributwerte enthält.

Sie verwenden diese Methode, um automatisch alle Ergebnisse oder alle Ergebnisse, die bestimmte Merkmale aufweisen, an einen Reaktions- oder Korrektur-Workflow zu senden.

> **Note**
>
> Sowohl Security Hub als auch Security Hub CSPM senden die Ergebnisse an die Adresse EventBridge unter der Quelle von. `aws.securityhub` Stellen Sie sicher, dass Ihre EventBridge Regeln den für Security Hub spezifischen Detailtyp verwenden, um doppelte Benachrichtigungen im Zusammenhang mit Security Hub CSPM-Ergebnissen zu vermeiden.

EventBridge Veranstaltungsformate

Der Findings Imported V2 Ereignistyp verwendet das folgende Eventformat.

Beispiel

Dieses Format wird verwendet, wenn Security Hub ein Ereignis an sendet EventBridge.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Findings Imported V2",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "e51603d1054aad9d9f498d82d6e81acf4cf6bc88140e8ad2273123c73b81084"
   ],
   "detail":{
      "findings": [{
```

```
          <finding content>
        }]
    }
}
```

Jedes Ereignis sendet ein einzelnes Ergebnis. *<finding content>*ist der Inhalt des vom Ereignis gesendeten Ergebnisses in JSON.

Eine vollständige Liste der Suchattribute finden Sie unter OCSF-Ergebnisse in Security Hub CSPM.

Regeln konfigurieren für EventBridge

Sie können in Amazon eine Regel erstellen EventBridge , die eine Aktion definiert, die ausgeführt werden soll, wenn ein Findings Imported V2 Ereignis eingeht. Findings Imported V2Ereignisse werden durch Aktualisierungen ausgelöst `BatchUpdateFindingsV2`.

Jede Regel enthält ein Ereignismuster, das die Ereignisse identifiziert, die die Regel auslösen. Das Ereignismuster enthält immer die Ereignisquelle (`aws.securityhub`) und den Ereignistyp (Findings Imported V2). Das Ereignismuster kann auch Filter angeben, um die Ergebnisse zu identifizieren, für die die Regel gilt.

Die Ereignisregel identifiziert dann die Regelziele. Bei den Zielen handelt es sich um die Aktionen, die ergriffen werden EventBridge müssen, wenn ein Findings Imported V2-Ereignis eingeht und das Ergebnis den Filtern entspricht.

Die hier bereitgestellten Anweisungen verwenden die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben in Amazon EventBridge Logs ermöglicht. CloudWatch

Sie können auch den `PutRule` Betrieb der API verwenden. EventBridge Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Informationen zur erforderlichen Richtlinie finden Sie unter CloudWatch Logs-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

Format des Ereignismusters

Das Format des Ereignismusters für Findings Imported V2-Ereignisse lautet wie folgt:

```
{
  "source": [
```

```
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifiziert Security Hub als den Dienst, der das Ereignis generiert.
- `detail-type`identifiziert die Art des Ereignisses.
- `detail`ist optional und stellt die Filterwerte für das Ereignismuster bereit. Wenn das Ereignismuster kein `detail` Feld enthält, lösen alle Ergebnisse die Regel aus.

Sie können die Ergebnisse anhand eines beliebigen Ergebnisattributs filtern. Für jedes Attribut geben Sie ein kommagetrenntes Array mit einem oder mehreren Werten an.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Wenn Sie mehr als einen Wert für ein Attribut angeben, werden diese Werte durch verknüpft. `OR` Ein Ergebnis entspricht dem Filter für ein einzelnes Attribut, wenn das Ergebnis einen der aufgelisteten Werte enthält. Wenn Sie beispielsweise `INFORMATIONAL` sowohl `LOW` als auch Werte für angeben`Severity.Label`, stimmt das Ergebnis überein, wenn es den Schweregrad entweder `INFORMATIONAL` oder hat`LOW`.

Die Attribute werden durch verknüpft`AND`. Ein Ergebnis stimmt überein, wenn es den Filterkriterien für alle angegebenen Attribute entspricht.

Wenn Sie einen Attributwert angeben, muss dieser die Position dieses Attributs innerhalb der AWS Open Cybersecurity Schema Framework (OCSF) -Struktur widerspiegeln.

Im folgenden Beispiel enthält das Ereignismuster Filterwerte für `ProductArn` und. Ein Ergebnis stimmt also überein`Severity.Label`, wenn es von Amazon Inspector generiert wurde und den Schweregrad entweder `INFORMATIONAL` oder `LOW` hat.

```
{
```

```
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Eine Ereignisregel erstellen

Sie können ein vordefiniertes Ereignismuster oder ein benutzerdefiniertes Ereignismuster verwenden, um eine Regel in zu erstellen EventBridge. Wenn Sie ein vordefiniertes Muster auswählen, füllt es EventBridge automatisch `source` und aus`detail-type`. EventBridge enthält auch Felder zur Angabe von Filterwerten für die folgenden Suchattribute:

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

Um eine EventBridge Regel zu erstellen (Konsole)

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Erstellen Sie mithilfe der folgenden Werte eine EventBridge Regel, die das Auffinden von Ereignissen überwacht:
   - Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
   - Wählen Sie aus, wie das Ereignismuster erstellt werden soll.

Um das Event-Muster zu erstellen mit...	Vorgehensweise	
Eine Vorlage	Wählen Sie im Abschnitt Event-Muster die folgenden Optionen aus: • Als Event source (Ereignisquelle) wählen Sie AWS -Services aus. • Wählen Sie für AWS Service Security Hub aus. • Wählen Sie als Ereignistyp die Option Findings Imported V2 aus. • (Optional) Fügen Sie Filterwerte hinzu, um die Regel spezifischer zu gestalten. Um die Regel beispielsweise auf Ergebnisse mit aktivem Datensatzstatus zu beschränken, wählen Sie für Bestimmte Datensatzstatus (e) die Option Aktiv aus.	

Um das Event-Muster zu erstellen mit...	Vorgehensweise
Ein benutzerdefiniertes Ereignismuster (Verwenden Sie ein benutzerdefiniertes Muster, wenn Sie Ergebnisse anhand von Attributen filtern möchten, die nicht in der EventBridge Konsole angezeigt werden.)	• Wählen Sie im Abschnitt Ereignismuster die Option Benutzerdefinierte Muster (JSON-Editor) aus, und fügen Sie dann das folgende Ereignismuster in den Textbereich ein: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }` • Aktualisieren Sie das Ereignismuster, sodass es das Attribut und die Attributwerte enthält, die Sie als Filter verwenden möchten. Um die Regel beispielsweise auf Ergebnisse mit einem Schweregrad von

Um das Event-Muster zu erstellen mit...	Vorgehensweise	
	anzuwendenCritical, verwenden Sie das folgende Musterbeispiel: `{ "source": ["aws.securityhub" ], "detail-type": ["Findings Imported V2"], "detail":{ "findings": { "Severity": ["Critical"] } } }`	

- Wählen Sie für Zieltypen die Option AWS Service aus, und wählen Sie für Wählen Sie ein Ziel aus, z. B. ein Amazon SNS-Thema oder eine AWS Lambda Funktion. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.

Einzelheiten zum Erstellen von Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren.

> **Note**
>
> Wenn Sie in Security Hub CSPM EventBridge Regeln für Ergebnisse definiert haben, können sich die Regeln mit den für Security Hub definierten Regeln überschneiden. Um zu vermeiden, dass doppelte Ergebnisse gesendet werden, überprüfen Sie die Regeln, die Sie für Security Hub CSPM definiert haben, um festzustellen, ob sie sich mit den Regeln

überschneiden, die Sie für Security Hub definiert haben. Deaktivieren Sie gegebenenfalls alle Security Hub CSPM-Regeln, die durch Security Hub-Regeln ersetzt wurden.

Ergebnisse von Security Hub nach Amazon S3 exportieren

Sie können Ergebnisse aus AWS Security Hub in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren, den Sie besitzen. Ein Export erfasst die Ergebnisse, die den Filtern auf der Seite entsprechen, von der aus Sie ihn starten, und schreibt sie als CSV-Datei oder als JSON im Format Open Cybersecurity Schema Framework (OCSF) in Ihren Bucket. Verwenden Sie Exporte, um Ergebnisse mit Teams zu teilen, die die Security Hub Hub-Konsole nicht verwenden, Ergebnisse in ein Data Warehouse oder ein Business Intelligence-Tool zu laden oder Point-in-Time-Aufzeichnungen für Audits zu führen.

Exporte sind auf Anfrage möglich. Sie starten einen Export, Security Hub führt ihn im Hintergrund aus und die Dateien werden in Ihrem Bucket angezeigt, wenn er abgeschlossen ist. Sie können jeden Export auf der Seite Exporte in der Security Hub Hub-Konsole verfolgen.

So funktioniert der Export von Ergebnissen

Sie starten einen Export auf einer der Ergebnisseiten in der Security Hub Hub-Konsole: Alle Ergebnisse, Exposure, Threats, Vulnerabilities, Sensitive Data oder Posture Management. Der Export verwendet die Seite als Gültigkeitsbereich und übernimmt die Filter, die Sie auf dieser Seite angewendet haben. Wenn Sie beispielsweise die Seite Sicherheitslücken nach kritischen Ergebnissen mit dem Status filtern`New`, enthält der Export nur diese Ergebnisse.

Security Hub schreibt den Export in den Amazon S3 S3-Bucket und das von Ihnen gewählte Präfix und verschlüsselt jedes Objekt mit dem von Ihnen AWS KMS ausgewählten Schlüssel AWS Key Management Service ().

> **Note**
>
> In einem Konto kann jeweils nur ein Export ausgeführt werden. Um einen weiteren Export zu starten, warten Sie, bis der laufende Export abgeschlossen ist, oder brechen Sie ihn auf der Seite Exporte ab.

Voraussetzungen

Bevor Sie einen Export erstellen, benötigen Sie einen Amazon S3 S3-Bucket, einen AWS KMS Schlüssel, Richtlinien für beide, die es Security Hub ermöglichen, in sie zu schreiben, und IAM-Berechtigungen für die Identität, die den Export erstellt.

Einen Export erstellen

Um einen Export zu erstellen

1. Öffnen Sie die Security Hub Hub-Konsole und wählen Sie die Ergebnisseite aus, von der Sie exportieren möchten: Alle Ergebnisse, Gefährdung, Bedrohungen, Sicherheitslücken, Vertrauliche Daten oder Statusverwaltung.
2. Wenden Sie die Filter an, die für den Export verwendet werden sollen.
3. Wählen Sie Export aus. Die Seite Export erstellen wird geöffnet.
4. Überprüfen Sie unter Umfang den Geltungsbereich. Es lautet Alle Ergebnisse und verwendet dabei die Filter, die von der Seite Sicherheitslücken übernommen wurden (oder der Name der Seite, von der Sie gekommen sind). Um den Geltungsbereich oder die Filter zu ändern, kehren Sie zur Ergebnisseite zurück und passen Sie sie dort an.

   Filter werden auf OCSF-Felder angewendet. Wenn ein Filter auf der Quellseite nicht auf Ergebnisse zutrifft, zeigt die Konsole eine Warnung mit den Namen der Filter an, die er nicht übernommen hat.
5. Gehen Sie unter Exporteinstellungen wie folgt vor:

   - Exportname — Geben Sie einen Namen ein, damit Sie den Export später in der Exportliste finden können. Die Konsole schlägt beispielsweise einen Namen vor, der aus der Quellseite und der aktuellen Uhrzeit erstellt wurde`vulnerabilities-202610081601`.
   - Exportformat — Wählen Sie CSV oder JSON (OCSF).
   - CSV-Spalten (nur CSV) — Jede Option zeigt den Spaltennamen und den OCSF-Feldpfad, aus dem sie stammt, zum Beispiel Finding account ()`cloud.account.uid`. Die Felder sind nach OCSF-Objekten gruppiert, z. B. Finding Info, Cloud, Resources, Compliance, Vulnerabilities und Evidences. Der Standardsatz enthält neun Spalten: Suchtitel, Schweregrad, Ressourcen-ID, Erstellt am, Status, Suchkonto, Suchregion, Name des Produktanbieters und Suchtyp.

     JSON-Exporte (OCSF) enthalten immer den vollständigen Befund, sodass keine Spalten ausgewählt werden müssen.

6. Wählen Sie unter Exportstandort Ihren Amazon S3 S3-Bucket aus und fügen Sie Ihren AWS KMS Schlüssel für die Verschlüsselung hinzu.
7. Wählen Sie Export erstellen.

Wenn in Ihrem Konto bereits ein Export ausgeführt wird, zeigt die Konsole das Dialogfeld Export läuft an. Sie können warten, bis der Export abgeschlossen ist, oder Sie können Export abbrechen und neu erstellen wählen, um den Export abzubrechen und diesen zu starten.

Third-party Integrationen für Security Hub

Sie können Ihre Sicherheitslage mit Integrationen von Drittanbietern für AWS Security Hub verbessern. Mit dieser Funktion können Sie Integrationen aktivieren, die Erkenntnisse von Security Hub nutzen, sodass Sie Ihre Betriebs-, Untersuchungs- und Reaktionstools in Security Hub integrieren können. Derzeit unterstützt Security Hub die Integration mit Jira Cloud undServiceNow.

Themen

- Integrationen für AWS Security Hub Jira Cloud
- Integrationen für ServiceNow
- Wichtige KMS-Richtlinien für Security Hub-Ticketing-Integrationen
- Testen konfigurierter Ticketing-Integrationen

Integrationen für AWS Security Hub Jira Cloud

In diesem Thema wird beschrieben, wie Sie Security Hub mit integrierenJira Cloud. Bevor Sie eines der Verfahren in diesem Thema abschließen können, müssen Sie ein Jira Cloud Abonnement erwerben. Informationen zu Abonnementplänen finden Sie auf der Atlassian Website unter Preise.

Diese Integration ermöglicht es Ihnen, Security Hub Hub-Ergebnisse manuell oder automatisch an Jira Cloud zu senden, sodass Sie sie als Teil Ihrer betrieblichen Workflows verwalten können. Sie können beispielsweise Problemen, die untersucht und behoben werden müssen, die Verantwortung zuweisen.

Für Konten in einer Organisation kann nur der delegierte Administrator eine Integration konfigurieren. Der delegierte Administrator kann die Funktion „Ticket erstellen“ manuell für alle Ergebnisse zu Mitgliedskonten verwenden. Darüber hinaus kann der delegierte Administrator mithilfe von Automatisierungsregeln automatisch Tickets für alle Ergebnisse im Zusammenhang mit

Mitgliedskonten erstellen. Bei der Definition einer Automatisierungsregel kann der delegierte Administrator Kriterien festlegen, die alle Mitgliedskonten oder bestimmte Mitgliedskonten umfassen können. Informationen zum Einrichten eines delegierten Administrators finden Sie unter Ein delegiertes Administratorkonto in Security Hub einrichten.

Für Konten, die nicht zu einer Organisation gehören, sind alle Aspekte dieser Funktion verfügbar.

Voraussetzungen

Bevor Sie Security Hub mit Ihrer Jira Cloud Umgebung verbinden, müssen Sie sicherstellen, dass die folgenden Konfigurationsschritte in Ihrer Jira-Umgebung ausgeführt werden.

- Installieren Sie die Cloud-App AWS Security Hub für Jira.
- Haben Sie mindestens ein Softwareentwicklungsprojekt, das vom Unternehmen verwaltet wird.
- Ordnen Sie die AWS App den Softwareentwicklungsprojekten zu, für die Sie Ergebnisse von Security Hub erhalten möchten.

Die Schritte für jede dieser Voraussetzungen sind unten aufgeführt.

1. Installieren Sie das AWS Security Hub für Jira Cloud App

Security Hub verfügt über eine App zur Unterstützung der Integration mit Jira. Diese App installiert benutzerdefinierte Felder und einen benutzerdefinierten Problemtyp. Security Hub verwendet diese, um bestimmte Attribute zu Ergebnissen zu füllen.

1. Melden Sie sich als Administrator Atlassian auf Ihrer Site an.
2. Wählen Sie Einstellungen und dann Apps.
3. Wenn Sie zur Marketplace-Seite weitergeleitet werden, wählen Sie Neue Apps suchen. Wenn Sie zur Apps-Seite weitergeleitet werden, wählen Sie Apps entdecken und suchen Sie dann nach AWS Security Hub für Jira Cloud. Wählen Sie dann Jetzt herunterladen.

2. Erstellen Sie ein Projekt oder überprüfen Sie bestehende Projekte

Dieser Schritt ist erforderlich, wenn Sie kein Projekt erstellt haben. Informationen zum Erstellen eines Projekts finden Sie in der Jira Cloud Support Dokumentation unter Neues Projekt erstellen.

Voraussetzungen für die Erstellung eines Projekts

Stellen Sie sicher, dass Sie beim Erstellen eines neuen Projekts Folgendes beachten.

- Wählen Sie Softwareentwicklung für die Projektvorlage aus.
- Wählen Sie Company-managedden Projekttyp aus.

Anforderungen für bestehende Projekte

Bei allen vorhandenen Projekten in Ihrer Jira-Umgebung, die in Security Hub integriert sind, muss es sich um einen Projekttyp von Company-managedhandeln.

3. Fügen Sie Ihre Projekte dem AWS Security Hub für Jira Cloud App

Damit Security Hub Ergebnisse erfolgreich an Ihre Jira-Umgebung senden kann, muss jedes Projekt, das Sie mit Security Hub verwenden möchten, mit dem AWS Security Hub für Jira Cloud App verknüpft sein. Durch die Verknüpfung eines Jira-Projekts mit der App wird sichergestellt, dass die erforderlichen benutzerdefinierten Felder für Security Hub dem Projekt zugeordnet sind und ausgefüllt werden können, wenn Security Hub Ergebnisse an das Projekt sendet.

1. Melden Sie sich als Administrator auf Ihrer Atlassian Site an.
2. Wählen Sie Einstellungen und dann Apps.
3. Wählen Sie in der Liste der Apps AWS Security Hub for Jira Cloud aus.
4. Wählen Sie den Tab Connector-Einstellungen.
5. Wählen Sie unter Aktivierte Projekte die Option Jira-Projekt hinzufügen aus.
    a. Wählen Sie in der Dropdownliste die Option Alle hinzufügen oder wählen Sie ein Projekt aus. Wiederholen Sie diesen Teil des Schritts, wenn Sie mehr als ein Projekt hinzufügen möchten, aber nicht alle Projekte.
    b. Wählen Sie Speichern.

Auf der Registerkarte Installation Manager können Sie überprüfen, welche Projekte erfolgreich installiert wurden. Auf der Registerkarte Installation Manager können Sie auch Konfigurationen für Felder, Bildschirme, Status und Workflows überprüfen.

Weitere Informationen Jira Cloud dazu finden Sie in den Jira CloudRessourcen auf der Atlassian Website.

Empfehlungen

Erstellen Sie ein spezielles Systemkonto für Ihre Jira-Umgebung

Die Security Hub Hub-Integration mit Jira Cloud verwendet eine OAuth-Verbindung, die einem bestimmten Benutzer in Ihrer Jira-Instanz zugeordnet ist. Aus den folgenden Gründen wird für Ihre Verbindung empfohlen, ein spezielles Systemkonto für Ihre Security Hub Hub-OAuth-Verbindung zu erstellen:

- Ein dedizierter Systembenutzer stellt sicher, dass die Verbindung nicht mit einem Mitarbeiter verknüpft ist, dessen Berechtigungen für die Jira-Umgebung sich im Laufe der Zeit ändern könnten, was die Integrationsfähigkeit von Security Hub in Ihre Jira-Umgebung beeinträchtigt.
- Bei jedem Problem, das Security Hub in Jira erstellt, wird ein Feld Erstellt von angezeigt, das den Benutzernamen enthält, der zum Erstellen der OAuth-Verbindung verwendet wurde. Die Verwendung eines Systemkontos für die OAuth-Verbindung führt dazu, dass dieses Systemkonto als Ticketersteller erscheint. Dadurch wird deutlich, dass das Ergebnis durch die Security Hub Hub-Integration und nicht manuell von einem anderen Jira-Benutzer erstellt wurde.

Konfigurieren Sie eine Integration zwischen Security Hub und Jira Cloud

Das folgende Verfahren muss für jedes Ihrer Jira Cloud Projekte abgeschlossen werden, an das Sie Security Hub Hub-Ergebnisse senden möchten.

> **Note**
>
> Wenn Sie einen Jira Cloud Connector erstellen, werden Sie vom aktuellen AWS-Region zu weitergeleitet`"https://3rdp.oauth.console.api.aws"`, sodass Sie die Connector-Registrierung abschließen können. Danach kehren Sie zu dem Ort zurück, AWS-Region an dem der Konnektor erstellt wird.

Um eine Integration zu konfigurieren für Jira Cloud

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.
2. Wählen Sie im Navigationsbereich Management und dann Integrationen aus.
3. Wählen Sie HinzufügenJira Cloud aus.
4. Geben Sie unter Details einen eindeutigen und aussagekräftigen Namen für Ihre Integration ein und legen Sie fest, ob Sie eine optionale Beschreibung für Ihre Integration eingeben möchten.
5. Wählen Sie unter Verschlüsselungen aus, wie Sie Ihre Anmeldeinformationen für die Integration in Security Hub verschlüsseln möchten.

- AWS Eigenen Schlüssel verwenden — Bei dieser Option wird ein eigener Serviceschlüssel von Security Hub verwendet, um Ihre Anmeldeinformationen für die Integration innerhalb von Security Hub zu verschlüsseln.
- Wählen Sie einen anderen KMS-Schlüssel (erweitert) — Mit dieser Option wählen Sie einen AWS KMS key , den Sie erstellt haben und den Sie für die Verschlüsselung Ihrer Integrationsdaten in Security Hub verwenden möchten. Informationen zum Erstellen eines AWS KMS Schlüssels finden Sie unter Create a AWS KMS key im AWS Key Management Service Developer Guide. Wenn Sie Ihren eigenen Schlüssel verwenden möchten, müssen Sie dem KMS-Schlüssel Richtlinienanweisungen hinzufügen, die Security Hub den Zugriff auf den Schlüssel ermöglichen. Einzelheiten zu den erforderlichen Richtlinien finden Sie in den AWS KMS wichtigsten Richtlinien für Security Hub-Ticketintegrationen.

> **Note**
>
> Sie können diese Einstellungen nicht mehr ändern, sobald Sie diese Konfiguration abgeschlossen haben. Wenn Sie jedoch Benutzerdefinierter Schlüssel wählen, können Sie Ihre benutzerdefinierte Schlüsselrichtlinie jederzeit bearbeiten.

6. (Optional) Erstellen Sie für Tags ein Tag und fügen Sie es Ihrer Integration hinzu. Sie können bis zu 50 Tags hinzufügen.
7. Wählen Sie für Autorisierungen die Option Connector erstellen und autorisieren aus. Es erscheint ein Pop-up, in dem Sie Zulassen wählen, um die Autorisierung abzuschließen. Nachdem Sie die Autorisierung abgeschlossen haben, wird ein Kontrollkästchen angezeigt, das Sie darüber informiert, dass die Autorisierung erfolgreich war.
8. Geben Sie für Konfigurationen die Jira Cloud Projekt-ID ein.
9. Wählen Sie Vollständige Konfiguration aus. Nachdem Sie die Konfiguration abgeschlossen haben, können Sie Ihre konfigurierten Integrationen auf der Registerkarte Konfigurierte Integrationen einsehen.

Nachdem Sie Ihre Integration mit Jira konfiguriert haben, können Sie die Verbindung testen, um sicherzustellen, dass in Ihrer Jira-Umgebung und in Security Hub alles richtig konfiguriert ist. Weitere Informationen finden Sie unter Testen konfigurierter Ticketing-Integrationen.

Zusätzliche Informationen zur Jira-Integration

Überlegungen zur Ratenbegrenzung

Jira setzt API-Ratenbegrenzungen durch, um die Servicestabilität aufrechtzuerhalten und eine faire Nutzung auf der gesamten Plattform zu gewährleisten. Bei Verwendung der AWS Security Hub Hub-Integration mit Jira können sich diese Ratenbegrenzungen auf die Verarbeitung von Security Hub Hub-Ergebnissen auswirken, insbesondere in Umgebungen, in denen große Mengen an Ergebnissen generiert werden. Dies kann zu einer verzögerten Ticketerstellung führen, und in Szenarien mit extrem hohem Ergebnisvolumen werden einige Ergebnisse möglicherweise überhaupt nicht in Jira-Tickets verarbeitet. Um Ihre Integration zu optimieren, sollten Sie in Erwägung ziehen, Filter für Automatisierungsregeln in Security Hub zu implementieren, um das Ticketing bei den wichtigsten Ergebnissen zu priorisieren, Ihre Jira-API-Nutzung über deren Admin-Konsole zu überwachen und Ihren Workflow auf der Grundlage der spezifischen Ratenlimits Ihrer Jira-Lizenzstufe zu planen. Wenden Sie sich bei geschäftskritischen Implementierungen an Ihren Jira-Administrator, um Ihre Zuteilungen von Ratenlimits zu überprüfen.

Ausführliche Informationen zu den Ratenlimits der Jira-API findest du in der Dokumentation zur Ratenbegrenzung auf der Website des Atlassian Developers Guide.

Authentifizierung und Sicherheit

Die Jira-API-Authentifizierung erfordert eine korrekte OAuth 2.0-Konfiguration für einen sicheren Zugriff. Stelle sicher, dass deine Anwendung den bewährten Sicherheitsmethoden von Atlassian für die API-Integration entspricht.

Ressourcen:

- Jira REST API v3: Jira REST API v3-Dokumentation auf der Atlassian-Website
- Implementierung von OAuth 2.0 (3LO): Leitfaden zur Implementierung von OAuth 2.0 (3LO) auf der Atlassian-Website
- Jira Cloud-Apps verwalten: Ressourcen für die Verwaltung von Jira Cloud auf der Atlassian-Website
- Jira-Berechtigungen verwalten: Projektberechtigungen auf der Atlassian-Website verwalten

Ein Ticket erstellen für ein Jira Cloud Integration

Nachdem Sie eine Integration mit erstellt habenJira Cloud, können Sie ein Ticket für einen Befund erstellen.

> **Note**
>
> Ein Ergebnis wird während seines gesamten Lebenszyklus immer einem einzelnen Ticket zugeordnet. Security Hub sendet alle nachfolgenden Aktualisierungen eines Befundes nach der ersten Erstellung an dasselbe Ticket. Wenn ein mit einer Automatisierungsregel verknüpfter Connector geändert wird, wird der aktualisierte Connector nur für neue und eingehende Ergebnisse verwendet, die den Regelkriterien entsprechen.

Um ein Ticket für einen Befund zu erstellen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie ein Ergebnis aus. Wählen Sie im Ergebnis die Option Ticket erstellen aus.
4. Öffnen Sie für Integration das Drop-down-Menü und wählen Sie eine Integration aus. Diese Integration ist die Integration, die Sie zuvor bei der Konfiguration des Jira Cloud Projekts erstellt haben. Wählen Sie die Integration aus, an die die Ergebnisse gesendet werden sollen.
5. Wählen Sie Erstellen aus.

Ein Ticket anzeigen für einen Jira Cloud Integration

Nachdem Sie ein Ticket für einen Befund erstellt haben, können Sie das Ticket auf Ihrer Jira Cloud Instanz öffnen.

Um einen Befund auf deinem anzusehen Jira Cloud Instance

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie die Suche aus, in der Sie das Ticket erstellt haben.
4. Wählen Sie in der Suche die Ticket-ID aus, um das Ticket auf Ihrer Jira Cloud Instanz anzuzeigen, oder wählen Sie „JSON anzeigen“ aus.

Integrationen für ServiceNow

In diesem Thema wird beschrieben, wie Sie auf die Security Hub Hub-Konsole zugreifen, um eine Integration für zu konfigurierenServiceNow ITSM. Bevor Sie eines der Verfahren in diesem Thema abschließen können, müssen Sie über ein Abonnement verfügen, ServiceNow ITSM bevor Sie diese Integration hinzufügen können. Weitere Informationen finden Sie auf der Seite mit den Preisen auf der ServiceNow Website.

Für Konten in einer Organisation kann nur der delegierte Administrator eine Integration konfigurieren. Der delegierte Administrator kann die Funktion „Ticket erstellen“ manuell für alle Ergebnisse zu Mitgliedskonten verwenden. Darüber hinaus kann der delegierte Administrator mithilfe von Automatisierungsregeln automatisch Tickets für alle Ergebnisse im Zusammenhang mit Mitgliedskonten erstellen. Bei der Definition einer Automatisierungsregel kann der delegierte Administrator Kriterien festlegen, die alle Mitgliedskonten oder bestimmte Mitgliedskonten umfassen können. Informationen zum Einrichten eines delegierten Administrators finden Sie unter Ein delegiertes Administratorkonto in Security Hub einrichten.

Für Konten, die nicht zu einer Organisation gehören, sind alle Aspekte dieser Funktion verfügbar.

Voraussetzungen — ServiceNow Umgebung konfigurieren

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie eine Integration für konfigurieren könnenServiceNow ITSM. Andernfalls funktioniert Ihre Integration zwischen ServiceNow ITSM und Security Hub nicht.

1. Installieren Sie die Security Hubfinds-Integration für IT Service Management (ITSM)

Das folgende Verfahren beschreibt, wie das Security Hub-Plugin installiert wird.

1. Melden Sie sich bei Ihrer ServiceNow ITSM Instance an und öffnen Sie dann den Anwendungsnavigator.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie nach Security Hub Findings Integration for IT Service Management (ITSM) und wählen Sie dann Get, um die Anwendung zu installieren.

> **Note**
>
> Wählen Sie in den Einstellungen für die Security Hub Hub-Anwendung aus, welche Aktion ausgeführt werden soll, wenn neue Security Hub Hub-Ergebnisse an Ihre ServiceNow ITSM

Umgebung gesendet werden. Sie können „Nichts tun“, „Vorfall erstellen“, „Problem erstellen“ oder „Beides erstellen“ wählen (incident/problem).

2. Konfigurieren Sie den Gewährungstyp für Client-Anmeldeinformationen für eingehende OAuth-Anfragen

Sie müssen diesen Gewährungstyp für eingehende OAuth-Anfragen konfigurieren. Weitere Informationen finden Sie auf der Support-Webseite unter Gewährungstyp für Kundenanmeldedaten für eingehendes OAuth wird unterstützt. ServiceNow

3. Erstellen Sie eine OAuth-Anwendung

Wenn Sie bereits eine OAuth-Anwendung erstellt haben, können Sie diese Voraussetzung überspringen. Informationen zum Erstellen einer OAuth-Anwendung finden Sie unter OAuth einrichten auf der Website. ServiceNow

Voraussetzungen — konfigurieren AWS Secrets Manager

Um die Integration von Security Hub mit nutzen zu können ServiceNow, müssen die Anmeldeinformationen für Ihre ServiceNow OAuth-Anwendung in Secrets Manager gespeichert sein. Wenn Sie Ihre Anmeldeinformationen in Secrets Manager speichern, haben Sie die Kontrolle und den Überblick über die Verwendung der Anmeldeinformationen und ermöglichen es Security Hub gleichzeitig, die Anmeldeinformationen für die Integration in Ihre ServiceNow Instance zu verwenden. Um Ihre Anmeldeinformationen in Secrets Manager zu speichern, müssen Sie einen vom Kunden verwalteten AWS KMS Schlüssel verwenden, um die Geheimnisse zu schützen. Mit diesem AWS KMS Schlüssel können Sie die Geheimnisse schützen, während sie im Ruhezustand gespeichert sind. Außerdem können Sie dem Schlüssel eine Richtlinie zuordnen, die Security Hub Zugriff auf den Schlüssel gewährt, der das Geheimnis schützt.

Gehen Sie wie folgt vor, um Secrets Manager für Ihre ServiceNow Anmeldeinformationen zu konfigurieren.

Schritt 1: Hängen Sie eine Richtlinie an Ihr an AWS KMS Schlüssel

Um Ihre ServiceNow Integration erfolgreich zu konfigurieren, müssen Sie Security Hub zunächst die Berechtigungen zur Verwendung des AWS KMS Schlüssels erteilen, der Ihren ServiceNow Anmeldeinformationen in Secrets Manager zugeordnet ist.

Um das zu ändern AWS KMS wichtige Richtlinie für den Zugriff auf Ihre ServiceNow Anmeldeinformationen durch Security Hub

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um die AWS Region zu ändern, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie einen vorhandenen AWS KMS Schlüssel aus oder führen Sie die Schritte zum Erstellen eines neuen Schlüssels im AWS KMS Entwicklerhandbuch aus.
4. Wählen Sie im Abschnitt Key policy (Schlüsselrichtlinie) die Option Edit (Bearbeiten) aus.
5. Wenn Zur Richtlinienansicht wechseln angezeigt wird, wählen Sie diese aus, um die Schlüsselrichtlinie anzuzeigen, und klicken Sie dann auf Bearbeiten.
6. Kopieren Sie den folgenden Richtlinienblock in Ihre AWS KMS Schlüsselrichtlinie, um Security Hub die Erlaubnis zur Verwendung Ihres Schlüssels zu erteilen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::your-account-id:root"
        },
        "Action": "kms:*",
        "Resource": "*"
        },
        {
        "Sid": "Allow Security Hub connector service to decrypt secrets",
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "kms:Decrypt",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
            "kms:ViaService": "secretsmanager.your-region.amazonaws.com"
            },
            "StringLike": {
```

```
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:your-
region:your-account-id:secret:ServiceNow*"
            }
        }
        }
    ]
    }
```

7. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte im Richtlinienbeispiel ersetzen:
   - *your-account-id*Ersetzen Sie es durch Ihre AWS Konto-ID.
   - *your-region*Ersetze es durch deine AWS Region (z. B.`us-east-1`).
8. Wenn Sie die Grundsatzerklärung vor der Schlusserklärung hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Erklärung ein Komma hinzu. Stellen Sie sicher, dass die JSON-Syntax Ihrer AWS KMS wichtigsten Richtlinie gültig ist.
9. Wählen Sie Speichern.
10. (Optional) Kopieren Sie den Schlüssel ARN auf einen Notizblock, um ihn in den späteren Schritten zu verwenden.

Schritt 2: Erstellen Sie das Geheimnis in Secrets Manager

Erstellen Sie in Secrets Manager ein Geheimnis, in dem Ihre ServiceNow Anmeldeinformationen gespeichert werden. Security Hub greift bei der Interaktion mit Ihrer ServiceNow Umgebung auf dieses Geheimnis zu.

Folgen Sie den Anweisungen zum Erstellen eines Geheimnisses im AWS Secrets Manager Benutzerhandbuch. Nachdem Sie Ihr Secret erstellt haben, kopieren Sie den Secret ARN, da Sie ihn für die Erstellung Ihres Security Hub Hub-Connectors benötigen.

Achten Sie bei der Erstellung des Secrets darauf, dass Sie Folgendes konfigurieren:

Typ des Geheimnisses

Other type of secret (Andere Art von Secret)

Key/value Paare (Klartext-Format)

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
```

```
    }
```

> **Note**
>
> Die Feldnamen müssen exakt `ClientId` und `ClientSecret` (Groß- und Kleinschreibung beachten) sein. Security Hub benötigt genau diese Namen, um die Anmeldeinformationen abzurufen.

Verschlüsselungsschlüssel

Verwenden Sie den AWS KMS Schlüssel, den Sie in Schritt 1 konfiguriert haben

Ressourcenrichtlinie

Verwenden Sie die folgende Ressourcenrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager:your-region:your-account-
id:secret:ServiceNow*",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "your-account-id",
            "aws:SourceArn": "arn:aws:securityhub:your-region:your-account-id:*"
            }
        }
        }
    ]
    }
```

Nachdem Ihr Secret konfiguriert ist, können Sie mithilfe der CreateConnector V2-API oder AWS -Konsole einen Security Hub Hub-Connector erstellen. Sie müssen Folgendes angeben:

- InstanceName: Ihre ServiceNow Instanz-URL (zum Beispiel`your-instance.service-now.com`)
- SecretArn: Der ARN des Secrets, das Sie in diesem Verfahren erstellt haben

Konfigurieren Sie eine Integration für ServiceNow ITSM

Security Hub kann Vorfälle oder Probleme automatisch in erstellenServiceNow ITSM.

Um eine Integration zu konfigurieren für ServiceNow ITSM

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.
2. Wählen Sie im Navigationsbereich Management und dann Integrationen aus.
3. Wählen Sie ServiceNow ITSMunter Integration hinzufügen aus.
4. Geben Sie unter Details einen Namen für Ihre Integration ein und legen Sie fest, ob Sie eine optionale Beschreibung für Ihre Integration eingeben möchten.
5. Wählen Sie unter Verschlüsselungen aus, wie Sie Ihre Anmeldeinformationen für die Integration in Security Hub verschlüsseln möchten.

    - Eigenen Schlüssel verwenden AWS — Bei dieser Option wird ein Security Hub-eigener Serviceschlüssel verwendet, um Ihre Integrationsanmeldedaten innerhalb von Security Hub zu verschlüsseln.
    - Wählen Sie einen anderen KMS-Schlüssel (erweitert) — Mit dieser Option wählen Sie einen AWS KMS key , den Sie erstellt haben und den Sie für die Verschlüsselung Ihrer Integrationsdaten in Security Hub verwenden möchten. Informationen zum Erstellen eines AWS KMS Schlüssels finden Sie unter Create a AWS KMS key im AWS Key Management Service Developer Guide. Wenn Sie Ihren eigenen Schlüssel verwenden möchten, müssen Sie dem KMS-Schlüssel Richtlinienanweisungen hinzufügen, die Security Hub den Zugriff auf den Schlüssel ermöglichen. Einzelheiten zu den erforderlichen Richtlinien finden Sie in den AWS KMS wichtigsten Richtlinien für Security Hub-Ticketintegrationen.

> **Note**
>
> Sie können diese Einstellungen nicht mehr ändern, sobald Sie diese Konfiguration abgeschlossen haben. Wenn Sie jedoch Benutzerdefinierter Schlüssel wählen, können Sie Ihre benutzerdefinierte Schlüsselrichtlinie jederzeit bearbeiten.

6. Geben Sie unter Anmeldeinformationen Ihre ServiceNow ITSM URL und den ARN Ihres AWS Secrets Manager Geheimnisses ein, der im Abschnitt Voraussetzungen generiert wurde.
7. Legen Sie für Tags fest, ob Sie ein optionales Tag erstellen und zu Ihrer Integration hinzufügen möchten.
8. Wählen Sie Add Integration (Integration hinzufügen) aus. Nachdem Sie die Konfiguration abgeschlossen haben, können Sie Ihre konfigurierten Integrationen auf der Registerkarte Konfigurierte Integrationen einsehen.

Nachdem Sie Ihre Integration mit konfiguriert haben ServiceNow, können Sie die Verbindung testen, um sicherzustellen, dass in Ihrer ServiceNow Umgebung und in Security Hub alles richtig konfiguriert ist. Weitere Informationen finden Sie unter Testen konfigurierter Ticketing-Integrationen.

Erstellen eines Tickets für ein ServiceNow ITSM Integration

Nachdem Sie eine Integration mit erstellt habenServiceNow ITSM, können Sie ein Ticket für einen Befund erstellen.

> **Note**
>
> Ein Ergebnis wird während seines gesamten Lebenszyklus immer mit einem einzigen Ticket verknüpft. Security Hub sendet alle nachfolgenden Aktualisierungen eines Befundes nach der ersten Erstellung an dasselbe Ticket. Wenn ein mit einer Automatisierungsregel verknüpfter Connector geändert wird, wird der aktualisierte Connector nur für neue und eingehende Ergebnisse verwendet, die den Regelkriterien entsprechen.

Um ein Ticket für einen Befund zu erstellen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.

2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie einen Befund aus. Wählen Sie im Ergebnis die Option Ticket erstellen aus.
4. Öffnen Sie für Integration das Drop-down-Menü und wählen Sie eine Integration aus.
5. Wählen Sie Erstellen aus.

Ein Ticket für einen anzeigen ServiceNow ITSM Integration

Nachdem Sie ein Ticket für einen Befund erstellt haben, können Sie das Ticket auf Ihrer ServiceNow ITSM Instanz öffnen.

Um einen Befund auf deinem zu sehen ServiceNow ITSM Instance

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie die Suche aus, in der Sie das Ticket erstellt haben.
4. Wählen Sie in der Suche die Ticket-ID aus, um das Ticket auf Ihrer ServiceNow ITSM Instanz anzuzeigen, oder wählen Sie „JSON anzeigen“ aus.

Wichtige KMS-Richtlinien für Security Hub-Ticketing-Integrationen

Wenn Sie kundenverwaltete KMS-Schlüssel mit Security Hub-Ticketing-Integrationen verwenden, müssen dem KMS-Schlüssel zusätzliche Richtlinien hinzugefügt werden, damit Security Hub mit dem Schlüssel interagieren kann. Darüber hinaus müssen Richtlinien hinzugefügt werden, die es dem Principal, der den Schlüssel zum Security Hub Connector hinzufügt, ermöglichen, auf den Schlüssel zuzugreifen.

Richtlinie für Security Hub-Berechtigungen

Die folgende Richtlinie beschreibt die Berechtigungen, die Security Hub benötigt, um auf den KMS-Schlüssel zugreifen und ihn verwenden zu können, der mit Ihrem Jira und Ihren ServiceNow Connectors verknüpft ist. Diese Richtlinie muss jedem KMS-Schlüssel hinzugefügt werden, der einem Security Hub-Connector zugeordnet ist.

Die Richtlinie enthält die folgenden Berechtigungen:

- Erlaubt Security Hub, Tokens, die für die Kommunikation mit Ihren Ticketing-Integrationen verwendet werden, mithilfe des Schlüssels zu schützen, vorübergehend darauf zuzugreifen oder sie zu aktualisieren. Die Berechtigungen sind durch den Bedingungsblock, der den Quell-ARN und den Verschlüsselungskontext überprüft, auf Vorgänge im Zusammenhang mit bestimmten Security Hub-Connectoren beschränkt.
- Ermöglicht Security Hub, Metadaten über den KMS-Schlüssel zu lesen, indem der `DescribeKey` Vorgang zugelassen wird. Diese Berechtigung ist erforderlich, damit Security Hub den Status und die Konfiguration des Schlüssels überprüfen kann. Der Zugriff ist durch die Quell-ARN-Bedingung auf bestimmte Security Hub-Konnektoren beschränkt.

```
{
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:Region:AccountId:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
```

```
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
            }
        }
}
```

Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte im Richtlinienbeispiel ersetzen:

- Ersetzen Sie *CloudProviderName* durch `JIRA_CLOUD` oder `SERVICENOW`
- *AccountId*Ersetzen Sie es durch die Konto-ID, unter der Sie den Security Hub-Connector erstellen.
- *Region*Ersetzen Sie durch Ihre AWS Region (z. B.`us-east-1`).

IAM-Prinzipalzugriff für den Security Hub-Betrieb

Jeder Principal, der einem Security Hub-Connector vom Kunden verwaltete KMS-Schlüssel zuweist, muss über Berechtigungen verfügen, um Schlüsseloperationen (Beschreiben, Generieren, Entschlüsseln, Neuverschlüsseln und Auflisten von Aliasen) für den Schlüssel, der dem Connector hinzugefügt wird, durchzuführen. Dies gilt für die V2- und V2-APIs. CreateConnector CreateTicket Die folgende Grundsatzerklärung sollte als Teil der Richtlinie für jeden Principal enthalten sein, der mit diesen APIs interagiert.

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
```

```
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        }
    }
}
```

Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte im Richtlinienbeispiel ersetzen:

- *RoleName*Ersetzen Sie es durch den Namen der IAM-Rolle, die Security Hub aufruft.
- Ersetzen Sie *CloudProviderName* durch `JIRA_CLOUD` oder `SERVICENOW`.
- *AccountId*Ersetzen Sie es durch die Konto-ID, unter der Sie den Security Hub-Connector erstellen.
- *Region*Ersetzen Sie durch Ihre AWS Region (z. B.`us-east-1`).

Testen konfigurierter Ticketing-Integrationen

Für konfiguriertes Jira und ServiceNow Integrationen können Sie die Verbindung testen, um sicherzustellen, dass die gesamte Konfiguration in Security Hub und in Ihrer Jira- oder Umgebung abgeschlossen ist. ServiceNow

Die Testticket-Funktion erstellt ein Ticket mit dem Titel. `TESTING Test CreateTicketV2 Finding` Das Testticket enthält Beispieldaten wie Konto-ID und Region des Kontos, in dem der Test durchgeführt wird, Beispielressourcendetails und ein Beispiel für AWS Finding JSON.

Testen von Integrationen mithilfe der Konsole

Verwenden Sie die folgenden Schritte, um Ihre Integration zu testen:

1. Wählen Sie im Security Hub-Navigationsbereich Integrationen aus.
2. Wählen Sie auf der Registerkarte Konfigurierte Integrationen die Integration aus, die Sie testen möchten.
3. Wählen Sie auf der Übersichtsseite für Ihre Integration die Option Testticket erstellen aus.
4. Security Hub zeigt eine Erfolgsmeldung und einen Link zum Testticket an, wenn der Test erfolgreich ist. Wenn der Test nicht erfolgreich ist, zeigt Security Hub einen Fehler an. Beheben Sie anhand der Fehlermeldung die Konfigurationsprobleme in Security Hub oder in Ihrer Jira ServiceNow OR-Umgebung.

> **Note**
>
> Die Testticket-Funktion soll Ihnen helfen, die vollständige Funktionalität beim Einrichten einer neuen Verbindung oder bei Änderungen an einer bestehenden Verbindung zu überprüfen. Diese Funktion erstellt jedes Mal, wenn sie verwendet wird, ein neues Ticket in Ihrer Jira oder Ihrer ServiceNow Umgebung und ist nicht für die regelmäßige Überprüfung Ihrer Verbindung vorgesehen.

Testen mit dem AWS CLI

Um Ihre Integration mit dem zu testen AWS CLI, verwenden Sie den `create-ticket-v2` Befehl mit dem `--mode DRYRUN` Parameter:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

Beispiel

Das folgende Beispiel zeigt, wie eine Integration getestet wird:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

Erfolgreiche Antwort

Eine erfolgreiche Antwort gibt Folgendes zurück:

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

`TicketSrcUrl`In der Antwort finden Sie einen direkten Link zum Anzeigen des Testtickets in Ihrem Jira oder Ihrer ServiceNow Umgebung.

Wenn der Test fehlschlägt, wird eine Fehlermeldung angezeigt, die auf das Konfigurationsproblem hinweist, das behoben werden muss.

Behebung von Fehlern bei der Jira Cloud-Integration

Wenn Sie Ihre Integration Jira Cloud von Security Hub aus testen, werden möglicherweise die folgenden Fehlermeldungen zurückgegeben. Diese Fehlermeldungen können Aufschluss darüber

geben, wo das Konfigurationsproblem mit dem Connector liegen könnte und wie es behoben werden kann.

Fehlermeldungen zur Jira Cloud-Integration

Fehler	Fehlermeldung	Wahrscheinliche Ursache und Lösung
ConflictException	Das Jira-Projekt kann nicht gefunden werden	Mögliche Ursache: Das Projekt auf dem Connector ist falsch oder ein credentials/permissions Problem, das uns daran hindert, auf das Projekt zuzugreifen. Wahrscheinliche Lösung: Füge das richtige Projekt zum Connector hinzu oder authentifiziere dich erneut mit den richtigen Anmeldeinformationen bei Jira.
ConflictException	Der Security Hub-Problemtyp wurde nicht gefunden	Mögliche Ursache: Das Problem bei der Installation der App oder der Problemtyp ist nicht mit dem Projekt verknüpft. Mögliche Lösung: Führen Sie den erforderlichen Schritt durch, um die Jira-App in Ihrer Jira-Umgebung zu installieren und die App mit dem Projekt zu verknüpfen.

MCP App (Vorschau)

Security Hub bietet ein agentisches Erlebnis mit einer Model Context Protocol (MCP) -App. Mit dieser App kann Ihr KI-Agent Expositionsergebnisse untersuchen. Es kann auch einen vorhandenen Azure-Connector diagnostizieren oder die Voraussetzungen für den Azure-Connector vor der Erstellung bewerten.

Bei jedem Aufruf des Ergebnistools wird eine Textzusammenfassung zurückgegeben, die der Agent zum Nachdenken verwenden kann. Wenn verfügbar, wird auch eine interaktive Visualisierung angezeigt, die Sie in derselben Konversation überprüfen können. Connector Diagnostics gibt strukturierten Text zurück, der bestätigte Ergebnisse von Prüfungen trennt, die nicht verifiziert werden konnten.

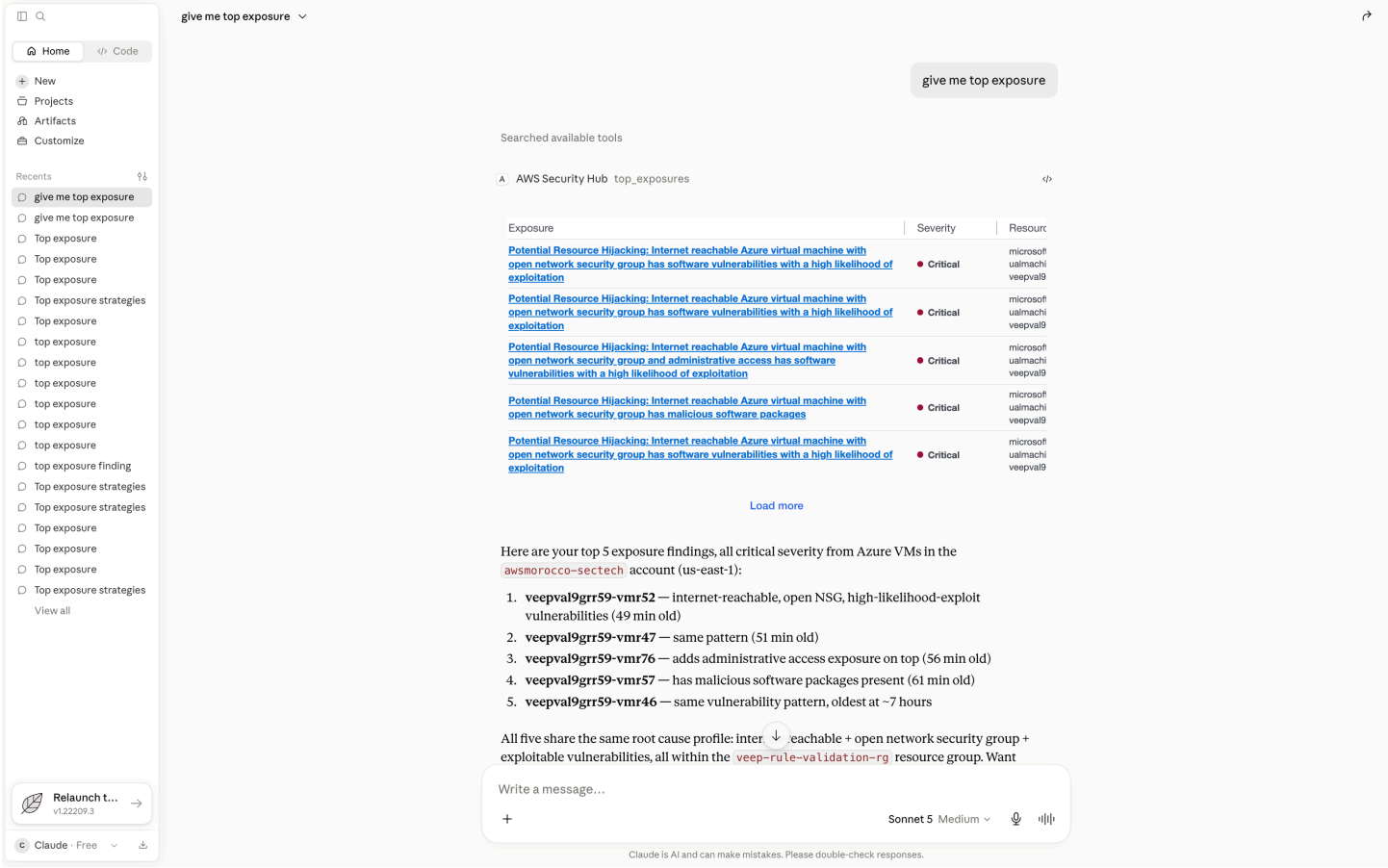
Die MCP-App ist ein lokaler MCP-Server, der auf Ihrem Computer ausgeführt wird und Security Hub-APIs direkt mit Ihren vorhandenen AWS Anmeldeinformationen aufruft. Connector Diagnostics kann auch begrenzte, schreibgeschützte Azure-CLI-Abfragen mithilfe Ihrer vorhandenen Azure-CLI-Sitzung ausführen. Jedes Tool ist schreibgeschützt und ändert nichts an Ihrer Sicherheitslage oder Ihren Connector-Ressourcen. Die MCP-App ist in allen AWS Handelsregionen verfügbar, in denen Security Hub verfügbar ist.

> **Important**
>
> Die Security Hub MCP-App befindet sich in der öffentlichen Vorschau.

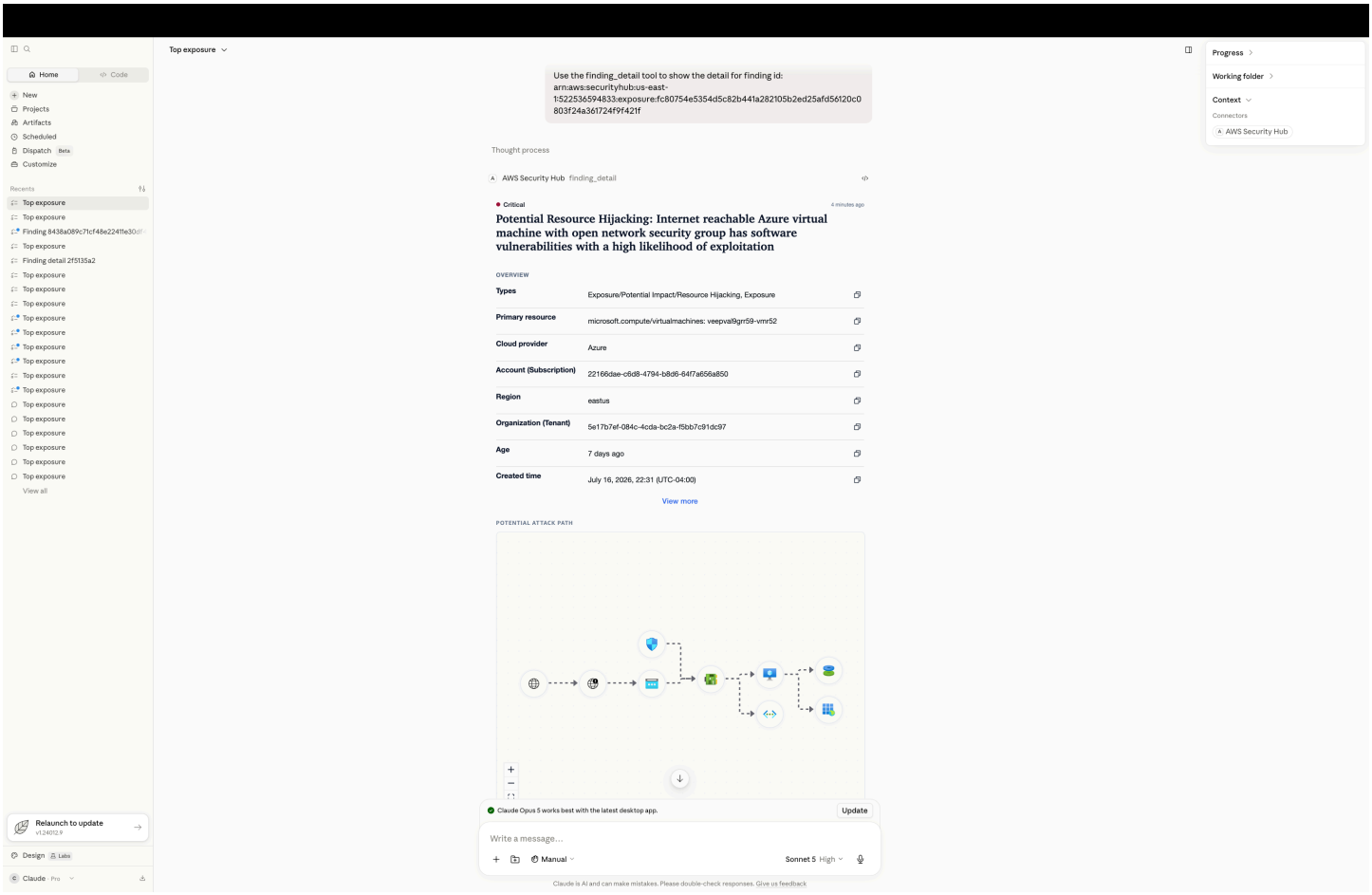
Beispiele für MCP-Apps

Die folgenden Beispiele zeigen, wie die MCP-App interaktive Visualisierungen in Claude Desktop rendert, während Sie Ihre Belichtungen untersuchen.

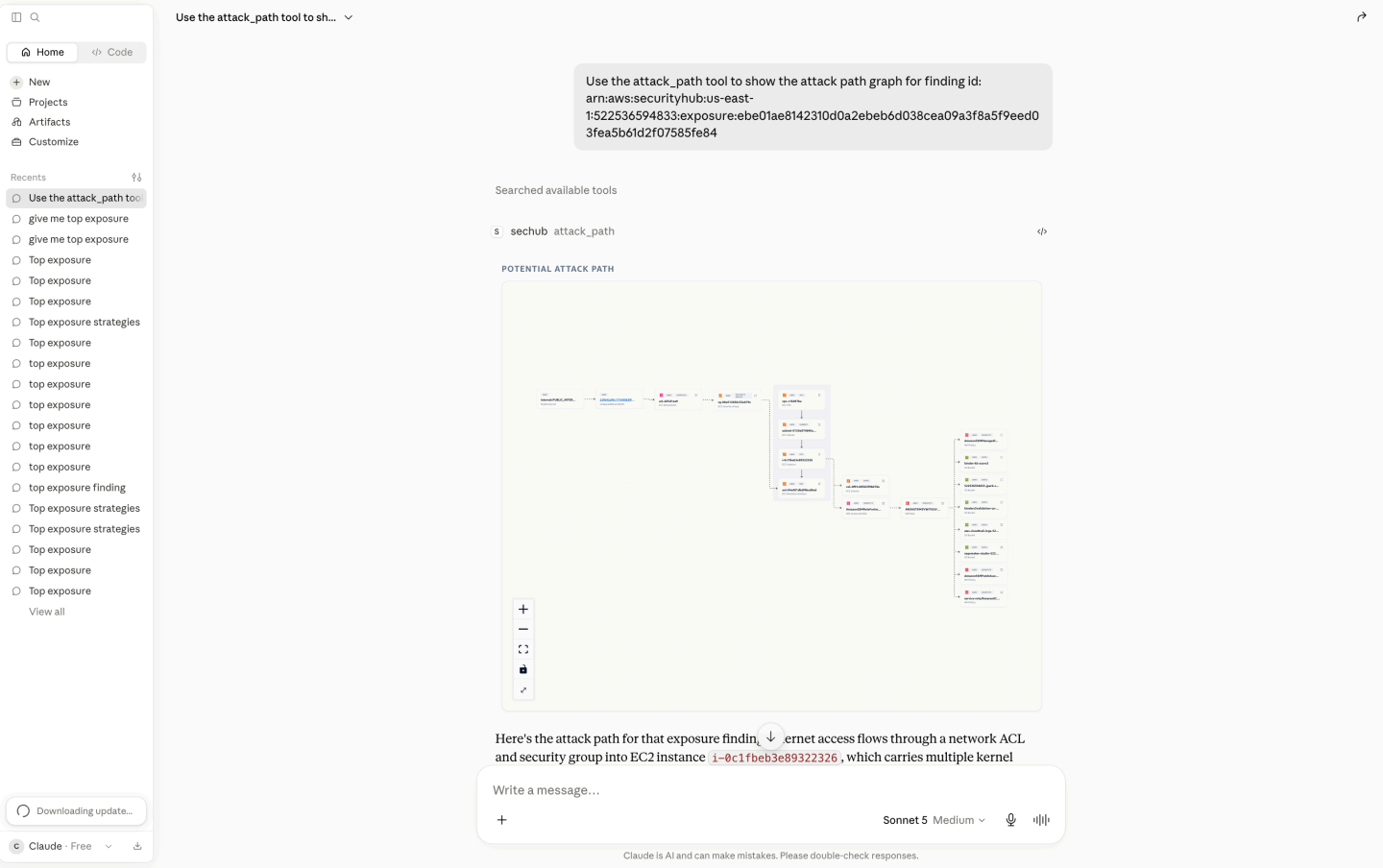
Häufigste Expositionen — Listet Ihre kritischsten Expositionsergebnisse in einer interaktiven Tabelle auf. Die folgende Abbildung zeigt die Tabelle mit den höchsten Expositionen.



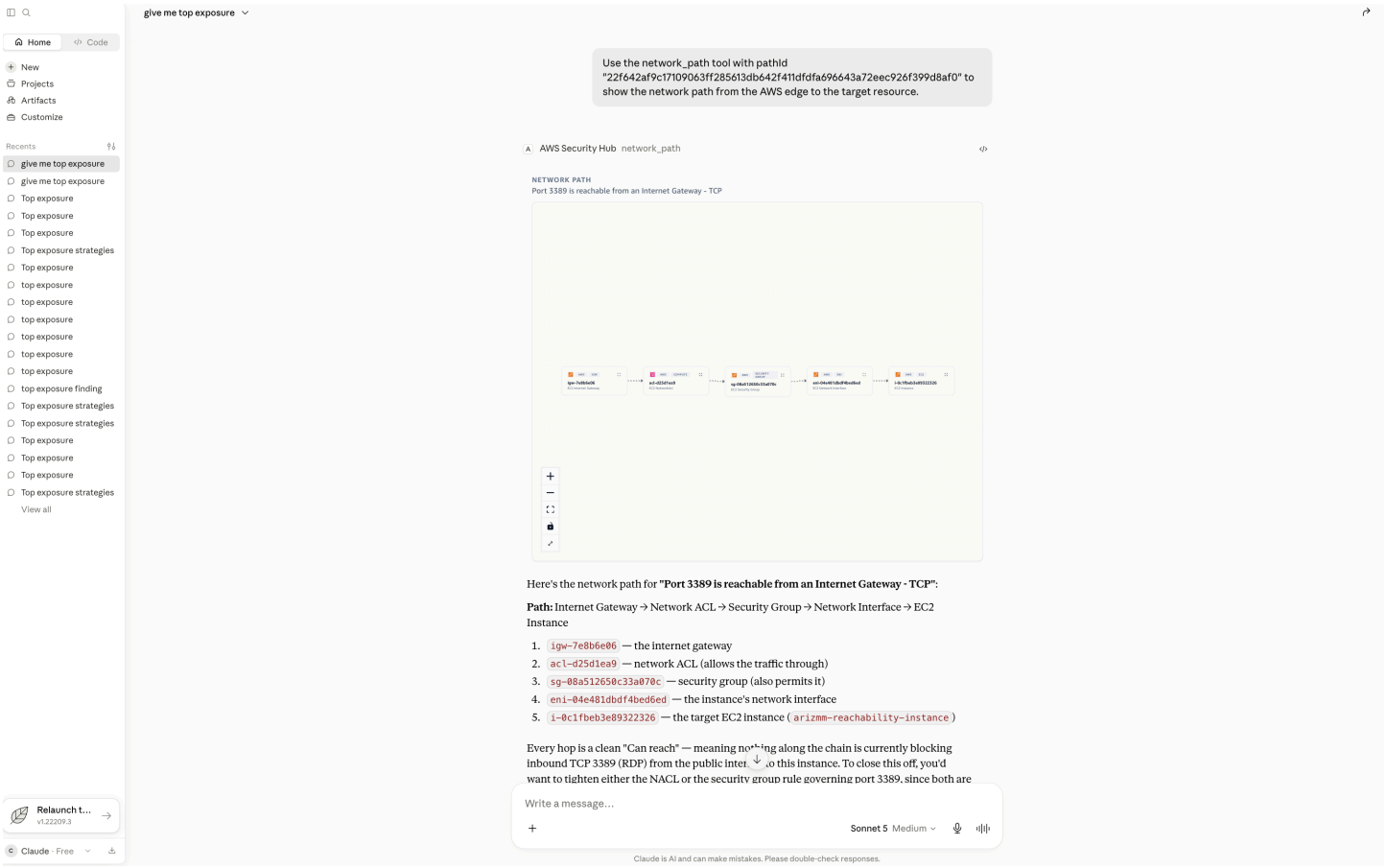
Einzelheiten zum Befund — Sehen Sie sich die Übersicht eines einzelnen Bedrohungsergebnisses zusammen mit einer Zusammenfassung der zugehörigen Erkennungsmerkmale, dem Angriffspfad und Anleitungen zur Behebung an. Die folgende Abbildung zeigt die Detailansicht der Ergebnisse.



Angriffspfad — Visualisieren Sie in einem interaktiven Diagramm, wie ein Risiko erreichbar ist. Knoten stehen für Ressourcen, Identitäten und Dienste. Kanten repräsentieren die Beziehungen zwischen ihnen. Das folgende Bild zeigt das Diagramm des Angriffspfads.



Netzwerkpfad — Erkunden Sie die geordneten Netzwerk-Hops vom AWS Edge zur Zielressource (z. B. Internet Gateway zu NACL zu Security Group zu ENI zu Instance). Die folgende Abbildung zeigt den Netzwerkpfad.



Connector-Diagnose — Fragen Sie, warum ein vorhandener Azure-Connector beeinträchtigt ist oder ausgefallen ist. Der Agent identifiziert bestätigte Probleme, unterscheidet Prüfungen, die nicht verifiziert werden konnten, und empfiehlt die kleinste Reparatur, ohne Ihre Umgebung zu verändern.

Connector-Bereitschaft — Prüfen Sie die Azure-Voraussetzungen, bevor Sie einen Connector erstellen. Der Agent meldet, welche Voraussetzungen erfüllt wurden, nicht bestanden haben oder nicht verifiziert werden konnten.

Die wichtigsten Konzepte

Gefährdungsermittlung — Ein Ergebnis, bei dem mehrere Signale — wie Sicherheitslücken, Fehlkonfigurationen, Netzwerkerreichbarkeit und vertrauliche Daten — zu einer einzigen Ansicht einer Ressource, die einem Risiko ausgesetzt ist, in Beziehung gesetzt werden.

Connector-Diagnose — Drei schreibgeschützte Tools für Azure-Connectors. Die Tools diagnostizieren einen vorhandenen Connector, bewerten eine vorgeschlagene Einrichtung und rufen genaue Auszüge aus dem unterstützten Azure-Setup-Skript ab. Der Agent wählt die Tools aus und übersetzt ihre strukturierten Ergebnisse in eine Erklärung.

Lokaler MCP-Server — Ein Programm, das auf Ihrem Computer ausgeführt wird und als sichere, bidirektionale Brücke zwischen Claude Desktop und Security Hub fungiert. Der Server enthält die Tools, die Ihr AI-Agent verwendet, einschließlich der Tools, die die Benutzeroberfläche in Claude Desktop rendern. Er verwendet die AWS Anmeldeinformationskette Ihres Computers und besitzt keine eigenen Anmeldeinformationen.

MCP-App — Eine interaktive Anwendung, die in Claude Desktop gerendert wird. Jede Ansicht der MCP-App erfüllt eine einzige Aufgabe, z. B. die Anzeige der Tabelle mit den höchsten Risiken oder eines Diagramms des Angriffspfads.

Doppelte Antwort — Ein einziger Aufruf des Tools für die Ergebnisse liefert zwei Ergebnisse: eine kompakte Textzusammenfassung, die Ihr Agent überlegt, und eine interaktive Visualisierung, die in derselben Konversation gerendert wurde, sodass Sie sie überprüfen können.

Voraussetzungen

- Ein AWS Konto, bei dem Security Hub aktiviert ist. Expositionsergebnisse sind nur für die Ergebnisse und Expositionsinstrumente erforderlich.
- Claude Desktop ist installiert. Das Installationsprogramm finden Sie im Claude Desktop-Download auf der Claude-Website.
- AWS Anmeldeinformationen, die in Ihrer AWS Standard-SDK-Anmeldeinformationskette konfiguriert sind.
- Installieren Sie für die Azure-side Connector-Diagnose die Azure-CLI. Authentifizieren Sie sich beim Mandanten des Connectors `az login --tenant`*`tenant-id`*, indem Sie Folgendes ausführen: Wo *`tenant-id`* ist die ID des Azure-Mandanten, der den Connector enthält. Die MCP-App verwendet die resultierende lokale Azure-CLI-Sitzung. Fügen Sie der MCP-Konfiguration keine Azure-Anmeldeinformationen hinzu.

> **Note**
>
> Sie können Connector Diagnostics ohne eine authentifizierte Azure-CLI-Sitzung ausführen. Das Ergebnis beinhaltet die verfügbare AWS Bewertung und markiert Azure-dependent Prüfungen als nicht verifiziert. Nicht verfügbare Azure-Beweise werden niemals als fehlerfrei behandelt.

Den MCP-Server einrichten

Die MCP-App wird in Claude Desktop aus einer Bundle-Datei installiert. Stellen Sie vor der Installation sicher, dass die Installation `aws sts get-caller-identity` erfolgreich ist und dass eine Region in Ihrem Terminal `aws configure get region` zurückgegeben wird, sodass der Server Ihre AWS Anmeldeinformationen und Ihre Region lesen kann.

1. Laden Sie das Security Hub MCP App-Paket herunter.
2. Öffnen Sie die heruntergeladene `.mcpb` Datei. Claude Desktop startet einen Konfigurationsablauf. Folgen Sie den Anweisungen, um den Server zu installieren.
3. Um die Verbindung zu überprüfen, geben Sie in Claude Desktop eine Frage ein, z. B. „Was sind meine wichtigsten Sicherheitsrisiken?“ oder „Mein Azure-Connector in us-west-2 ist herabgestuft. Können Sie feststellen, was falsch ist?“ Wenn Sie eine Fehlermeldung erhalten, lesen Sie die Hinweise in der Fehlermeldung und bestätigen Sie Ihre Anmeldedaten und Ihre Region.

Connector Diagnostics verwenden

Beschreiben Sie das Connector-Problem oder die vorgeschlagene Einrichtung in natürlicher Sprache. Der Agent wählt das entsprechende schreibgeschützte Tool aus, interpretiert das strukturierte Ergebnis und teilt Ihnen mit, welche Prüfungen bestätigt wurden und welche nicht.

Diagnostizieren Sie einen vorhandenen Connector

1. Identifizieren Sie den Stecker anhand seiner Connector-ID oder seines genauen Namens. Geben Sie auch das AWS Konto und die Region an, die den Connector enthalten, falls der Agent sie anhand Ihrer Anfrage nicht ermitteln kann.
2. Stellen Sie eine Frage wie „Mein Azure-Connector in us-west-2 ist herabgestuft. Können Sie feststellen, was falsch ist, und mir sagen, was zuerst behoben werden muss?“
3. Prüfen Sie die bestätigten Ergebnisse getrennt von den Prüfungen, die nicht verifiziert wurden. Wenn die Azure-Authentifizierung nicht verfügbar ist, beschränkt der Agent seine Schlussfolgerungen auf AWS direkte Beweise.

Beurteilen Sie einen vorgeschlagenen Konnektor

1. Geben Sie das AWS Konto, die AWS Region und die Azure-Mandanten-ID an. Geben Sie außerdem 1—10 Azure-Abonnement-IDs an, die der vorgeschlagene Connector abdecken wird.

Teilen Sie dem Agenten mit, welche Dienstvoraussetzungen geprüft werden müssen: Cloud Security Posture Management (CSPM), Inspector VM-Scanning oder Bedrohungserkennung. Diese Auswahl umfasst die Bereitschaftsprüfungen. Es handelt sich nicht um Einstellungen zur Konnektorerstellung.

2. Stellen Sie eine Frage wie „Bevor ich meinen Azure-Connector erstelle, überprüfen Sie, ob die Voraussetzungen für diese Abonnements erfüllt sind.“
3. Überprüfen Sie die bestandenen, fehlgeschlagenen und nicht verifizierten Prüfungen. Ein einwandfreies Bereitschaftsergebnis bedeutet, dass die geprüften Voraussetzungen erfüllt wurden. Das bedeutet nicht, dass ein Connector existiert, läuft oder wiederhergestellt wurde.

Rufen Sie die Installationsanweisungen ab

Wenn sich ein Ergebnis auf einen Onboarding-Schritt bezieht, bitten Sie den Agenten, diesen Schritt zu zeigen. Fragen Sie beispielsweise „Zeige mir Schritt 6 aus dem unterstützten Azure-Connector-Setupskript“. Das vollständige Skript finden Sie unter Konfiguration von Microsoft Azure für die Integration mit Security Hub. Das Tool gibt einen exakten Auszug zurück, führt ihn aber nicht aus. Führen Sie das gesamte unterstützte Skript aus, da seine Schritte die Konfiguration und die Hilfsfunktionen gemeinsam nutzen.

> **Note**
>
> Connector Diagnostics repariert oder verändert niemals Ressourcen. Bei der Problembehebung handelt es sich um eine Anleitung für eine separate Aktion, die Sie steuern. Bei der Diagnose wird eine Wiederherstellung nur gemeldet, wenn neue Laufzeitnachweise dies belegen.

Verfügbare Tools

`top_exposures`— Listet Ihre dringendsten Expositionsbefunde in einer interaktiven Tabelle auf. Rufen Sie dieses Tool zuerst auf, da für die Suchfunktionen eine Such-ID aus dieser Liste erforderlich ist.

`finding_detail`— Gibt den Überblick über ein Ergebnis zurück, einschließlich der Zusammenfassung der zugehörigen Ergebnismerkmale.

`finding_overview`— Gibt eine Textzusammenfassung eines Ergebnisses anhand der Such-ID zurück.

`correlated_finding_detail`— Listet die Ergebnisse auf, die einem Risiko für ein einzelnes Merkmal zugeordnet sind, z. B. Sicherheitslücke, Fehlkonfiguration oder Erreichbarkeit.

`attack_path`— Erstellt das Diagramm des Angriffspfads für ein Ergebnis.

`network_path`— Erweitert den Netzwerkpfad eines Finds um geordnete Sprünge vom AWS Rand zur Zielressource.

`recommendation`— Gibt Anleitungen zur Behebung eines Befundes zurück, einschließlich Links zur Dokumentation.

`resource_detail`— Gibt die Konfiguration einer AWS Ressource nach Kurz-ID (z. B.`i-1234`) oder ARN zurück.

`diagnose_connector`— Diagnostiziert einen vorhandenen Azure-Connector mithilfe des Security Hub-Status und begrenzter Azure-CLI-Nachweise, sofern verfügbar. Es werden bestätigte Ergebnisse, der betroffene Umfang, Anleitungen zur Problembehebung und die Aktualität der Daten zurückgegeben. Außerdem werden alle Prüfungen aufgeführt, die nicht verifiziert werden konnten.

`assess_connector_readiness`— Prüft vor der AWS Erstellung die Seite und Azure-side die Voraussetzungen für einen vorgeschlagenen Azure-Connector. Es wird kein Connector erstellt.

`get_connector_setup_instructions`— Gibt exakte Auszüge aus dem verpackten, unterstützten Azure-Onboarding-Skript zurück. Das Skript wird nicht ausgeführt.

Überwachung der Nutzung und der Kosten in Security Hub

Die Seite „Nutzung“ hilft Ihnen, die Kosten für den Betrieb von Security Hub in Ihrer Organisation zu verstehen und zu verwalten. Auf dieser Seite können Sie Ihre aktuellen Kosten und die voraussichtlichen monatlichen Kosten einsehen, die Nutzung nach Funktionen oder Konten untersuchen und Strategien zur Optimierung Ihrer Ausgaben finden.

Wer kann auf die Seite „Nutzung“ zugreifen

Die Nutzungsseite ist von jedem Konto aus verfügbar, für das Security Hub aktiviert ist. Um darauf zuzugreifen, öffnen Sie die Security Hub-Konsole und wählen Sie im Navigationsbereich unter Einstellungen die Option Nutzung aus.

> **Important**
>
> Wenn es sich bei Ihrem Konto um ein Mitgliedskonto in einer AWS Organisation handelt und kein delegierter Security Hub-Administrator benannt wurde, sind keine Nutzungsdaten verfügbar. Um Nutzungsdaten einsehen zu können, muss das Verwaltungskonto Ihrer Organisation einen delegierten Administrator benennen. Weitere Informationen finden Sie unter the section called “Benennung eines delegierten Administrators”.

Die Erfahrung ist je nach Kontotyp unterschiedlich:

- Delegierter Administrator oder Verwaltungskonto — Sie sehen die vollständige Nutzungsseite mit einer Übersicht über die Unternehmenskosten, Nutzung nach Funktionen, Nutzung nach Konto und Strategien zur Kostenoptimierung.
- Mitgliedskonto oder eigenständiges Konto — Es wird eine Übersicht der Kontokosten angezeigt, die nur für Ihr Konto die Nutzung nach Funktionen enthält. Der Tab Nach Konto ist nicht verfügbar, da Sie nur ein einziges Konto anzeigen.

Übersicht der Organisations- und Kontokosten

> **Note**
>
> Der Abschnitt mit der Zusammenfassung der Organisationskosten ist nur vom Konto des delegierten Administrators oder vom Verwaltungskonto aus sichtbar. Mitgliedskonten und Einzelkonten wird stattdessen eine Übersicht der Kontokosten angezeigt.

Wenn Sie die Seite „Nutzung“ von einem delegierten Administrator- oder Verwaltungskonto aus öffnen, wird im Abschnitt „Übersicht über die Organisationskosten“ eine allgemeine Übersicht der Security Hub-Kosten Ihres Unternehmens für den aktuellen Abrechnungszeitraum angezeigt. Dieser Abschnitt umfasst Folgendes:

- Letzte Aktualisierung der Daten — Das Datum, an dem Security Hub die Nutzungsdaten für Ihr Unternehmen zuletzt aktualisiert hat. Security Hub aktualisiert diese Daten regelmäßig. Wenn die Daten beim Aufrufen der Nutzungsseite älter als 24 Stunden sind, löst Security Hub automatisch eine Aktualisierung aus. Die Aktualisierung ist je nach Größe Ihrer Organisation innerhalb weniger

Stunden abgeschlossen. Während die Daten aktualisiert werden, wird eine Warnung mit der Meldung angezeigt, dass die Daten in Kürze verfügbar sein werden.

- Aktuelle Kosten — Der Gesamtbetrag, der Ihrem Unternehmen für die Nutzung von Security Hub vom Beginn des aktuellen Abrechnungszeitraums bis zum Datum der letzten Aktualisierung der Daten entstanden ist.
- Voraussichtliche monatliche Kosten (30 Tage) — Geschätzte monatliche Kosten auf der Grundlage der letzten 7 Tage der Nutzung, hochgerechnet auf einen vollen 30-tägigen Abrechnungszeitraum. Diese Prognose beinhaltet sowohl die kostenpflichtige als auch die kostenlose Testnutzung, sodass Sie eine realistische Schätzung Ihrer monatlichen Kosten erhalten. In den voraussichtlichen Kosten sind keine Rabatte (EDPs) enthalten, mit AWS denen Sie ausgehandelt haben. Wenn Ihre voraussichtlichen Kosten niedriger zu sein scheinen als Ihre aktuellen Kosten, bedeutet das, dass Ihre Nutzung gesunken ist. Basierend auf den letzten 7 Tagen der Nutzung wird die 30-Tage-Rechnung niedriger sein als Ihre Rechnung im aktuellen Abrechnungszeitraum.

Funktionsansicht

In der Capability-Ansicht werden Ihre Kosten und Ihre Nutzung im gesamten Unternehmen angezeigt, geordnet nach Sicherheitsfunktionen. Die Funktionen sind in drei erweiterbare Gruppen unterteilt. Sie können jede Gruppe erweitern oder reduzieren, um die einzelnen Nutzungstypen darin zu sehen. Jeder Nutzungstyp wird direkt einem entsprechenden Nutzungstyp im AWS Cost Explorer zugeordnet.

Security Hub Essentials Plan — Überwacht Ihre EC2-Instances, ECR-Container-Images, Lambda-Funktionen, IAM-Benutzer und IAM-Rollen. Deckt Risiko- und Risikoanalysen, Schwachstellenmanagement (unterstützt von Amazon Inspector), Sicherheitsmanagement (unterstützt von Security Hub CSPM) und Sicherheitsreaktionen ab. All diese Funktionen sind im Essentials-Tarif zu einem Preis pro Ressource enthalten. Sie müssen Amazon Inspector oder AWS Security Hub CSPM nicht separat aktivieren oder bezahlen, und die zugrunde liegende Servicenutzung wird Ihnen nicht doppelt berechnet.

Bedrohungsanalysen — Beinhaltet CloudTrail Verwaltungsereignisse und Datenereignisse, Netzwerkaktivitäten und andere Protokolle. Diese Funktionen umfassen die Bedrohungserkennung, die von Amazon bereitgestellt wird GuardDuty.

Zusätzliche Funktionen — Beinhaltet den Codescan für Lambda-Funktionen. Dies ist eine optionale Erweiterung, die von Amazon Inspector bereitgestellt wird, um den Anwendungscode der Lambda-Funktion auf Sicherheitslücken zu analysieren.

Weitere Informationen zur Preisgestaltung für die einzelnen Funktionen finden Sie unter Preise für Security Hub.

Die Tabelle in dieser Ansicht enthält die folgenden Spalten für jeden Nutzungstyp:

- Aktuelle Nutzung — Das gesamte Nutzungsvolumen für diesen Nutzungstyp vom Beginn des Abrechnungszeitraums bis zum Datum der letzten Aktualisierung der Daten für alle Konten und alle Regionen.
- Kostenlose Nutzung — Das gesamte Nutzungsvolumen für diesen Nutzungstyp aus Konten, die sich derzeit in der kostenlosen Testversion befinden. Die Werte für die kostenlose Nutzung werden grün angezeigt.
- Aktuelle Kosten — Die Gesamtkosten für diesen Nutzungstyp vom Beginn des Abrechnungszyklus bis zum Datum der letzten Aktualisierung der Daten für alle Konten und alle Regionen.
- Wert der kostenlosen Testversion — Die Kosten, die Ihnen für diesen Nutzungstyp entstanden wären, wenn die Konten, die sich derzeit in der kostenlosen Testversion befinden, nicht in der Testversion enthalten gewesen wären. Dies hilft Ihnen, den Wert der kostenlosen Testversion zu verstehen.
- Voraussichtliche monatliche Kosten (30 Tage) — Die geschätzten monatlichen Kosten für diesen Nutzungstyp, hochgerechnet aus den letzten 7 Tagen der Nutzung für alle Konten und alle Regionen. Dies beinhaltet sowohl die kostenpflichtige als auch die kostenlose Testnutzung, sodass die geschätzten monatlichen Kosten berechnet werden.

Kontoansicht

> **Note**
>
> Die Kontoansicht ist nur über das delegierte Administratorkonto oder das Verwaltungskonto verfügbar.

Wählen Sie die Kontoansicht, um Ihre Kosten nach einzelnen Mitgliedskonten in allen Regionen geordnet anzuzeigen. Anhand dieser Ansicht können Sie ermitteln, welche Konten die meisten Kosten verursachen.

In der Tabelle sind alle Konten mit den folgenden Spalten aufgeführt:

- Konto — Die AWS-Konto ID, die als anklickbarer Link angezeigt wird. Wenn Sie ein Konto auswählen, wird ein detailliertes Aufschlüsselungsfeld geöffnet.
- Aktuelle Kosten — Die Gesamtkosten für dieses Konto vom Beginn des Abrechnungszyklus bis zum Datum der letzten Aktualisierung der Daten in allen Regionen.
- Wert der kostenlosen Testversion — Die Kosten, die für dieses Konto entstanden wären, wenn es nicht in der kostenlosen Testversion enthalten gewesen wäre.
- Voraussichtliche monatliche Kosten (30 Tage) — Die geschätzten monatlichen Kosten für dieses Konto, hochgerechnet aus den letzten 7 Tagen der Nutzung in allen Regionen auf einen vollen 30-tägigen Abrechnungszeitraum. Die Prognose beinhaltet sowohl die kostenpflichtige als auch die kostenlose Testnutzung, sodass Sie eine repräsentative Schätzung Ihrer monatlichen Kosten erhalten. Die voraussichtlichen Kosten berücksichtigen keine Rabatte, mit denen Sie ausgehandelt haben AWS (EDVs).

  Wenn Security Hub innerhalb der letzten 7 Tage für dieses Konto aktiviert wurde, basiert die Prognose auf der Anzahl der Tage seit der Aktivierung. Nach 7 Tagen nutzt die Projektion die volle Nutzungsdauer der letzten 7 Tage. Auf der Nutzungsseite wird derzeit nicht erkannt, wann Security Hub für ein Konto deaktiviert wurde. Wenn Security Hub kürzlich für ein oder mehrere Konten deaktiviert wurde, werden diese Konten weiterhin in der Prognose angezeigt, bis sie nicht mehr verwendet werden. Warten Sie 7 Tage, nachdem Sie diese Änderungen vorgenommen haben, bis die Prognose den aktuellen Stand Ihrer Organisation widerspiegelt.

Ansicht der Kontodetails

Wenn Sie ein Konto aus der Liste auswählen, wird rechts auf der Seite ein Detailbereich geöffnet. In diesem Bereich wird dieselbe Aufschlüsselung nach Funktionsebenen wie in der Funktionsansicht angezeigt, allerdings nach dem jeweiligen Konto gefiltert. Sie können die aktuelle Nutzung, die kostenlose Nutzung, die aktuellen Kosten, den Wert der kostenlosen Testversion und die voraussichtlichen monatlichen Kosten für jeden Nutzungstyp innerhalb dieses Kontos in allen Regionen einsehen.

Strategien zur Kostenoptimierung

Wählen Sie auf der Seite „Nutzung“ Strategien zur Kostenoptimierung aus, um zu einer speziellen Seite mit umsetzbaren Möglichkeiten zu gelangen, Ihre Kosten zu verwalten und gleichzeitig Ihren Sicherheitsschutz aufrechtzuerhalten.

Jede Strategie wird als eigenständige Option präsentiert, die Sie je nach den Bedürfnissen Ihres Unternehmens evaluieren und anwenden können. Optionen ohne Sicherheitskompromisse werden zuerst aufgeführt. Nachdem Sie eine Strategie angewendet haben, dauert es in der Regel 24 bis 48 Stunden, bis Änderungen in Ihrer Abrechnung berücksichtigt werden.

Zugehörige Ressourcen

- Preise für Security Hub
- AWS Cost Explorer-Benutzerhandbuch

Security Hub deaktivieren

Security Hub für ein einzelnes Konto deaktivieren

Wenn Ihr Konto nicht Teil einer Organisation ist, können Sie Security Hub jederzeit in der Security Hub-Konsole deaktivieren oder die DisableSecurityHubV2 API verwenden. Wenn Sie Security Hub deaktivieren, werden keine Ergebnisse von Erkennungsmodulen mehr aufgenommen. Außerdem verlieren Sie den Zugriff auf vorhandene Ergebnisse, Integrationen und Konfigurationen.

Wenn Sie Security Hub für Ihr Konto in allen Regionen deaktivieren, löscht Security Hub auch den mit dem Dienst verknüpften IAM Access Analyzer, der bei der Aktivierung des Dienstes erstellt wurde. Wenn das automatische Löschen fehlschlägt, können Sie den Analyzer löschen, indem Sie den IAM Access Analyzer-API-Vorgang aufrufen. `DeleteServiceLinkedAnalyzer` Dieser Vorgang ist erst erfolgreich, nachdem Security Hub für Ihr Konto vollständig deaktiviert wurde. Wenn Sie Security Hub in einer einzelnen Region deaktivieren, aber in anderen Regionen weiterhin aktiviert sind, wird die Analyse ungenutzter Zugriffe weiterhin ausgeführt und die Ergebnisse werden weiterhin in Ihren verbleibenden aktivierten Regionen repliziert.

So deaktivieren Sie Security Hub

1. Melden Sie sich mit Ihren Anmeldedaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Allgemein aus.
3. Wählen Sie in Security Hub die Option Deaktivieren aus. Geben Sie **`Disable`** im Popup-Fenster das Wort ein und wählen Sie Deaktivieren.

Security Hub unternehmensweit deaktivieren

Wenn Sie der delegierte Administrator für eine AWS Organisation sind, haben Sie zwei Möglichkeiten, Security Hub für alle Mitgliedskonten zu deaktivieren.

Option 1: Security Hub mit Erkennungsmodulen deaktivieren

Sie können die Security Hub-Bereitstellung (grundlegende und zusätzliche Funktionen) und die Richtlinie aus dem Richtlinienkatalog in Ihrem delegierten Administratorkonto nutzen, um Security Hub zusammen mit Amazon Inspector für bestimmte Organisationseinheiten, Konten oder Regionen zu deaktivieren.

Um Security Hub und Amazon Inspector mithilfe einer Richtlinie für alle Mitgliedskonten zu deaktivieren

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.
3. Wählen Sie Security Hub (grundlegende und zusätzliche Funktionen) aus dem Konfigurationskatalog aus.
4. Geben Sie auf der Seite Security Hub konfigurieren im Abschnitt Details einen Namen und eine Beschreibung für die Richtlinie ein (z. B. „Security Hub Disablement Policy“).
5. Wählen Sie im Abschnitt Kontoauswahl eine der folgenden Optionen aus. Wählen Sie Alle Organisationseinheiten und Konten, wenn Sie die Deaktivierung auf alle Organisationseinheiten und Konten anwenden möchten. Wählen Sie Bestimmte Organisationseinheiten und Konten, wenn Sie die Deaktivierung auf bestimmte Organisationseinheiten und Konten anwenden möchten. Wenn Sie diese Option wählen, verwenden Sie die Suchleiste oder den Organisationsstrukturbaum, um die Zielorganisationseinheiten und Konten anzugeben.
6. Wählen Sie im Abschnitt Regionen die Option Alle Regionen deaktivieren aus, um Security Hub in allen Regionen zu deaktivieren. Wählen Sie optional, ob neue Regionen automatisch deaktiviert werden sollen. Wählen Sie „Regionen angeben“, um auszuwählen, welche spezifischen Regionen Sie deaktivieren möchten.
7. (Optional) Informationen zu den erweiterten Einstellungen finden Sie in der Anleitung von AWS Organizations.
8. (Optional) Fügen Sie für Ressourcen-Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Konfiguration leichter identifizieren können.

9. Wählen Sie Weiter aus.
10. Überprüfen Sie Ihre Änderungen und wählen Sie dann Anwenden. Ihre Zielkonten werden auf der Grundlage der Richtlinie konfiguriert. Der Konfigurationsstatus Ihrer Richtlinie wird oben auf der Seite „Richtlinien“ angezeigt.

Amazon GuardDuty deaktivieren und AWS Security Hub CSPM

Für GuardDuty und Security Hub CSPM-Funktionen müssen Sie die Funktionen in den jeweiligen delegierten Administratorkonten manuell deaktivieren. GuardDuty und Security Hub CSPM verwenden Bereitstellungen (einmalige Aktionen) anstelle von Richtlinien. Daher muss die Deaktivierung manuell von den jeweiligen Konsolen aus durchgeführt werden.

Option 2: Nur Security Hub deaktivieren

Wenn Sie bereits eine Security Hub-Richtlinie haben und nur Security Hub deaktivieren möchten, ohne Amazon Inspector oder Security Hub CSPM zu beeinträchtigen GuardDuty, gehen Sie wie folgt vor.

Um Security Hub nur für Mitgliedskonten zu deaktivieren

1. Melden Sie sich mit Ihrem AWS Konto mit Ihren delegierten Administratoranmeldedaten an. Öffnen Sie die Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/v2/home.
2. Wählen Sie im Navigationsbereich Management und dann Configurations aus.
3. Wählen Sie eine Ihrer Security Hub-Richtlinien aus den konfigurierten Richtlinien aus.
4. Wählen Sie Richtlinie bearbeiten und wählen Sie im Abschnitt Kontoauswahl eine der folgenden Optionen aus. Wählen Sie Alle Organisationseinheiten und Konten aus, wenn Sie die Deaktivierung auf alle Organisationseinheiten und Konten anwenden möchten. Wählen Sie Bestimmte Organisationseinheiten und Konten, wenn Sie die Deaktivierung auf bestimmte Organisationseinheiten und Konten anwenden möchten. Wenn Sie diese Option wählen, verwenden Sie die Suchleiste oder den Organisationsstrukturbaum, um die Zielorganisationseinheiten und Konten anzugeben.
5. Wählen Sie im Abschnitt Regionen die Option Alle Regionen deaktivieren aus, um Security Hub in allen Regionen zu deaktivieren. Wählen Sie optional, ob neue Regionen automatisch deaktiviert werden sollen. Wählen Sie „Regionen angeben“, um auszuwählen, welche spezifischen Regionen Sie deaktivieren möchten.

6. (Optional) Informationen zu den erweiterten Einstellungen finden Sie in den Anleitungen von AWS Organisationen.
7. (Optional) Fügen Sie für Ressourcen-Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Konfiguration leichter identifizieren können.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie Ihre Änderungen und wählen Sie dann Anwenden. Ihre Zielkonten werden auf der Grundlage der Richtlinie konfiguriert. Der Konfigurationsstatus Ihrer Richtlinie wird oben auf der Seite „Konfigurationen“ angezeigt.

Auswirkungen auf andere Sicherheitsdienste

Die Deaktivierung von Security Hub über eine Security Hub-Richtlinie hat keine Auswirkungen auf die Konfigurationen von Security Hub GuardDuty, CSPM und Amazon Inspector.

Wenn Sie Amazon Inspector nur für Mitgliedskonten deaktivieren müssen, können Sie die Vulnerability Management-Richtlinie aus dem Security Hub-Konfigurationskatalog verwenden. Navigieren Sie zur Security Hub-Konfigurationsseite, wählen Sie Vulnerability Management in Amazon Inspector aus und erstellen Sie eine Deaktivierungsrichtlinie, indem Sie die Schritte befolgen, die dem obigen Verfahren zur Deaktivierung von Security Hub ähneln.

Sicherheit beiAWSSecurity Hub

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWSbietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-partyAuditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWSCompliance-Programme. Informationen zu den Compliance-Programmen, die für Security Hub gelten, finden Sie unter AWSServices in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Security Hub anwenden können. In den folgenden Themen erfahren Sie, wie Sie Security Hub so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Security Hub Hub-Ressourcen zu überwachen und zu sichern.

Topics

- Datenschutz in AWS Security Hub
- AWS Identitäts- und Zugriffsmanagement für Security Hub
- Konformitätsüberprüfung für AWS Sicherheitszentrum
- Resilienz in AWS Sicherheitszentrum
- Infrastruktursicherheit in AWS Sicherheitszentrum
- AWS Security Hub und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Datenschutz in AWS Security Hub

Das AWS Modell der gilt für den Datenschutz in AWS Security Hub. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.

- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Security Hub oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Security Hub ist ein Serviceangebot für mehrere Mandanten. Um Ihre Daten zu schützen, verschlüsselt Security Hub ruhende Daten und Daten, die zwischen Komponentendiensten übertragen werden.

Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

> **Note**
>
> Diese Dokumentationsseite gilt nur für den erweiterten AWS Security Hub, der am 2. Dezember 2025 eingeführt wurde. Wenn Sie Kunde des ursprünglichen AWS Security Hubs (jetzt AWS Security Hub CSPM) sind, gilt die unten beschriebene Datennutzung erst, nachdem Sie den erweiterten AWS Security Hub aktiviert haben.

Sie können sich dafür entscheiden, dass Ihre Daten (in den Security Hub-Servicebedingungen als „Security Hub-Inhalte“ definiert) für die Entwicklung und Verbesserung von Security Hub und anderen AWS AWS Sicherheitsdiensten verwendet werden, indem Sie die Opt-Out-Richtlinie für AWS Organisationen verwenden. Sie können sich auch dann abmelden, wenn Security Hub solche Inhalte derzeit nicht erfasst. Weitere Informationen zur Deaktivierung finden Sie in den Opt-Out-Richtlinien für KI-Services im Benutzerhandbuch für AWS Organizations .

> **Note**
>
> Damit Sie die Opt-Out-Richtlinie verwenden können, müssen Ihre AWS Konten zentral von AWS Organisationen verwaltet werden. Falls Sie noch keine Organisation für Ihre AWS Konten erstellt haben, finden Sie weitere Informationen unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch.

Opt-Out hat folgende Auswirkungen:

- Security Hub löscht die Inhalte, die es zur Serviceverbesserung gesammelt und gespeichert hat, bevor Sie sich abmelden (falls vorhanden).
- Nach Ihrer Abmeldung wird Security Hub diese Inhalte nicht mehr zu Zwecken der Serviceverbesserung erheben oder speichern.

Im folgenden Abschnitt wird erläutert, wie Security Hub mit Ihren Inhalten zur Serviceverbesserung umgeht.

AWS Datennutzung von Security Hub

Derzeit sammelt oder speichert AWS Security Hub keine Security Hub-Inhalte zur Serviceverbesserung. In Zukunft kann Security Hub jedoch Sicherheitserkenntnisse Dritter, die Sie in Security Hub und anderen Formen von Security Hub-Inhalten (die Security Hub von Ihnen oder von vorgelagerten Diensten zur Bereitstellung von Security Hub-Funktionen erhält) zusammenfassen und verwenden, um Security Hub und andere AWS Sicherheitsdienstfunktionen zu verbessern.

Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität. Wenn Security Hub in Zukunft mit der Erfassung von Security Hub-Inhalten zur Serviceverbesserung beginnt, wird diese Seite aktualisiert, um diesen Änderungen Rechnung zu tragen und Einzelheiten darüber zu enthalten, welche Daten erfasst und wie sie verwendet werden. Sie können sich jederzeit von der Erfassung dieser Security Hub-Inhalte abmelden, indem Sie die oben beschriebene Opt-Out-Richtlinie für AWS Organisationen verwenden. Weitere Informationen zu AWS Datenschutzpraktiken finden Sie unter Häufig gestellte Fragen zum Datenschutz.

Referenzen

Ähnliche Opt-Out-Verfahren in anderen AWS Sicherheitsdiensten finden Sie unter:

- https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-opting-out-using-data.htmlIm GuardDuty Amazon-Benutzerhandbuch können Sie sich gegen die Verwendung Ihrer Daten zur Serviceverbesserung entscheiden.
- https://docs.aws.amazon.com/security-lake/latest/userguide/opting-out-of-using-your-data.htmlIm Amazon Security Lake-Benutzerhandbuch können Sie sich gegen die Verwendung Ihrer Daten zur Serviceverbesserung entscheiden.

So verwendet Security Hub Daten, um die von Ihnen aktivierten Funktionen bereitzustellen

Wenn Sie AWS Security Hub aktivieren, wird ein Hinweis angezeigt, in dem erklärt wird, dass Security Hub auf Daten zugreifen und diese verwenden kann, auf die es bereits Zugriff hat, um die Funktionen zu aktivieren, die Sie aktivieren möchten. Dieser Hinweis existiert, weil Security Hub darauf ausgelegt ist, im Laufe der Zeit zu wachsen und sich zu verbessern. Ständig werden neue Erkennungs-, Korrelations- und Anreicherungsfunktionen hinzugefügt, und viele davon stützen sich auf Daten (wie Ergebnisse, Konfigurationsdaten und andere Inhalte oder Metadaten), auf die Security Hub im Rahmen Ihrer bestehenden Einrichtung bereits Zugriff hat. Anstatt Sie jedes Mal zu bitten, sich anzumelden, wenn wir eine Möglichkeit zur Nutzung von Daten einführen, auf die Sie Security Hub bereits Zugriff gewährt haben, erhalten Sie mit dieser Mitteilung im Voraus einen klaren Überblick darüber, wie dieser Zugriff genutzt werden kann (jetzt und im Zuge der Weiterentwicklung des Dienstes).

In der Praxis bedeutet dies, dass die Aktivierung einer Security Hub-Funktion Ihre Anweisung an Security Hub ist, die relevanten Inhalte und Metadaten zu verwenden, die sich bereits in seiner Reichweite befinden, um die Funktionalität dieser Funktion bereitzustellen. Wenn eine von Ihnen aktivierte Funktion einen bestimmten Datentyp noch nicht vollständig nutzt, kann sich dies ändern, wenn wir Verbesserungen einführen. Beispielsweise könnte eine bestehende Funktion damit beginnen, zusätzlichen Kontext (z. B. Signale zur Geschäftskritik) einzubeziehen, um die Genauigkeit zu verbessern oder Ihnen tiefere Einblicke zu bieten, ohne dass Ihnen zusätzliche Kosten entstehen. Sie müssen keine neuen Maßnahmen ergreifen, damit diese Verbesserungen wirksam werden, da sie im Rahmen des Datenzugriffs funktionieren, den Sie bereits durch die Aktivierung von Security Hub und seinen Funktionen eingerichtet haben.

Dieser Ansatz ist darauf ausgelegt, Ihre Erfahrung zu verbessern, indem Security Hub den Wert der Funktionen, die Sie bereits aktiviert haben, kontinuierlich steigert, ohne dass es zu Problemen durch wiederholte Zustimmungen oder Konfigurationsanfragen für schrittweise Verbesserungen kommt. Dennoch behalten Sie die Kontrolle: Sie können Ihre Security Hub-Integrationen und aktivierten

Funktionen jederzeit über die Security Hub-Konsole überprüfen, verwalten oder deaktivieren. Diese bestimmt, auf welche Daten Security Hub in Zukunft zugreifen und welche Daten Security Hub verwenden kann.

AWS Identitäts- und Zugriffsmanagement für Security Hub

AWS Identity and Access Management (IAM) ist ein Programm AWS-Service , das einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Security Hub-Ressourcen zu nutzen. IAM ist ein Dienst AWS-Service , den Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Security Hub mit IAM
- Identity-based politische Beispiele für AWS Security Hub
- Service-linked Rollen für AWS Security Hub
- AWSverwaltete Richtlinien für Security Hub
- Fehlerbehebung AWS Identität und Zugriff auf den Security Hub

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Rolle:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung AWS Identität und Zugriff auf den Security Hub).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Security Hub mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based politische Beispiele für AWS Security Hub).

Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich AWS mit Ihren Identitätsdaten an. Sie müssen als IAM-Benutzer oder als IAM-Benutzer authentifiziert sein, indem Sie eine IAM-Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich mit Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen als Verbundidentität anmelden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Stellt für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen bereit. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, menschliche Benutzer dazu zu verpflichten, einen Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen darauf zuzugreifen.

Bei einer Verbundidentität handelt es sich um einen Benutzer aus Ihrem Unternehmensverzeichnis, einem Web-Identitätsanbieter oder Directory Service einem Benutzer, der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Verwenden Sie für eine zentrale Zugriffsverwaltung. AWS IAM Identity Center Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Es hat sich bewährt, temporäre Anmeldeinformationen anstelle von IAM-Benutzern

mit langfristigen Anmeldeinformationen zu verwenden. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer einen Verbund mit einem Identitätsanbieter verwenden, um AWS mithilfe temporärer Anmeldeinformationen auf den Zugriff zuzugreifen.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder eine AWS API-Operation aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie einer Identität oder Ressource zugeordnet sind. AWS wertet diese Richtlinien aus, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können integrierte Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximale Anzahl von Berechtigungen festgelegt werden kann, die von gängigeren Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen komplizierter zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Logik zur Richtlinienauswertung.

So funktioniert Security Hub mit IAM

Bevor Sie AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf AWS Security Hub zu verwalten, erfahren Sie, welche IAM-Funktionen für Security Hub verfügbar sind.

IAM-Funktionen, die Sie mit verwenden können AWS Sicherheits-Hub

IAM-Feature	Unterstützung für Security Hub
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Ja
Zugriffskontrolllisten (ACLs)	Nein
Attribute-based Zugriffskontrolle (ABAC) — Schlagworte in Richtlinien	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein

IAM-Feature	Unterstützung für Security Hub
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie Security Hub und andere AWS-Services Funktionen mit den meisten IAM-Funktionen funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch.

Identity-based Richtlinien für Security Hub

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Security Hub unterstützt identitätsbasierte Richtlinien. Weitere Informationen finden Sie unter Identity-based politische Beispiele für AWS Security Hub.

Resource-based Richtlinien für Security Hub

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Principals können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Security Hub unterstützt keine ressourcenbasierten Richtlinien. Sie können eine IAM-Richtlinie nicht direkt an eine Security Hub-Ressource anhängen.

Richtlinienaktionen für Security Hub

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu gewähren.

Richtlinienaktionen in Security Hub verwenden vor der Aktion das folgende Präfix:

```
securityhub:
```

Um beispielsweise einem Benutzer die Berechtigung zur Aktivierung von Security Hub zu gewähren. Dabei handelt es sich um eine Aktion, die dem `EnableSecurityHubV2` Betrieb der Security Hub-API entspricht, nehmen Sie die `securityhub:EnableSecurityHubV2` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Security Hub definiert seine eigenen Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

```
"Action": "securityhub:EnableSecurityHubV2"
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Beispiel:

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

Sie können auch mehrere Aktionen mithilfe von Platzhaltern (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

```
"Action": "securityhub:Get*"
```

Als bewährte Methode sollten Sie jedoch Richtlinien erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die zum Ausführen einer bestimmten Aufgabe erforderlich sind.

Eine Liste der Security Hub-Aktionen finden Sie unter Von AWS Security Hub definierte Aktionen in der Referenz zur Serviceautorisierung. Beispiele für Richtlinien, die Security Hub-Aktionen spezifizieren, finden Sie unterIdentity-based politische Beispiele für AWS Security Hub.

Richtlinien-Ressourcen für Security Hub

Unterstützt Richtlinienressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Security Hub definiert die folgenden Ressourcentypen:

- Hub (Hub)
- Produkt
- Finding-Aggregator, auch als regionsübergreifender Aggregator bezeichnet
- Automatisierungsregel

Sie können diese Arten von Ressourcen in Richtlinien mithilfe von ARNs angeben.

Eine Liste der Security Hub-Ressourcentypen und die jeweilige ARN-Syntax finden Sie unter Von AWS Security Hub definierte Ressourcen in der Serviceautorisierungsreferenz. Informationen

darüber, welche Aktionen Sie für die einzelnen Ressourcentypen angeben können, finden Sie unter Von AWS Security Hub definierte Aktionen in der Serviceautorisierungsreferenz. Beispiele für Richtlinien, die Ressourcen angeben, finden Sie unterIdentity-based politische Beispiele für AWS Security Hub.

Schlüssel für Richtlinien-Bedingungen für Security Hub

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Alle AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Security Hub-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Security Hub in der Serviceautorisierungsreferenz. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Security Hub definierte Aktionen. Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unterIdentity-based politische Beispiele für AWS Security Hub.

Zugriffskontrolllisten (ACLs) in Security Hub

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Security Hub unterstützt keine ACLs, was bedeutet, dass Sie einer Security Hub-Ressource keine ACL hinzufügen können.

Attribute-based Zugriffskontrolle (ABAC) mit Security Hub

Unterstützt ABAC (Tags in Richtlinien): Ja

Attribute-based Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags

an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Principals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Sie können Tags an Security Hub-Ressourcen anhängen. Sie können den Zugriff auf Ressourcen auch kontrollieren, indem Sie Tag-Informationen im `Condition` Element einer Richtlinie angeben.

Informationen zum Taggen von Security Hub-Ressourcen finden Sie unterKennzeichnen von Security Hub Hub-Ressourcen. Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf eine Ressource anhand von Tags steuert, finden Sie unter. Identity-based politische Beispiele für AWS Security Hub

Verwenden temporärer Anmeldeinformationen mit Security Hub

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen den kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS API-Operationen wie AssumeRole oder aufrufen GetFederationToken.

Security Hub unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Security Hub weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen anruft AWS-Service, zusammen mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Beispielsweise sendet Security Hub FAS-Anfragen an Downstream, AWS-Services wenn Sie Security Hub in Security Hub integrieren AWS Organizations und wenn Sie das delegierte Security Hub-Administratorkonto für eine Organisation unter Organisationen festlegen.

Für andere Aufgaben verwendet Security Hub eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unterService-linked Rollen für AWS Security Hub.

Servicerollen für Security Hub

Security Hub übernimmt oder verwendet keine Servicerollen. Um Aktionen in Ihrem Namen auszuführen, verwendet Security Hub eine dienstbezogene Rolle. Einzelheiten zu dieser Rolle finden Sie unterService-linked Rollen für AWS Security Hub.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu Betriebsproblemen bei Ihrer Nutzung von Security Hub führen. Bearbeiten Sie die Servicerollen nur, wenn Security Hub Sie dazu auffordert.

Service-linked Rollen für Security Hub

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstgebundene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Security Hub verwendet eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unterService-linked Rollen für AWS Security Hub.

Identity-based politische Beispiele für AWS Security Hub

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Security Hub Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder AWS API ausführen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien
- Die Security Hub Hub-Konsole verwenden
- Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen
- Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Security Hub Hub-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer

Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Die Security Hub Hub-Konsole verwenden

Um auf die AWS Security Hub Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Security Hub Hub-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie nicht wie vorgesehen.

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass diese Benutzer und Rollen die Security Hub Hub-Konsole verwenden können, fügen Sie der Entität auch die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Security Hub Hub-Ergebnisse einzusehen.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
```

```
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Security Hub Hub-Automatisierungsregeln zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer ein Security Hub-Administrator sein. Um Berechtigungen einzuschränken — z. B. um einem Benutzer zu erlauben, nur Automatisierungsregeln einzusehen — können Sie die Berechtigungen zum Erstellen, Aktualisieren und Löschen entfernen.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRuleV2"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:ListAutomationRulesV2",
                "securityhub:GetAutomationRuleV2"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteAutomationRuleV2"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked Rollen für AWS Security Hub

AWS Security Hub verwendet eine dienstverknüpfte AWS Identity and Access Management (IAM) - Rolle mit dem Namen. `AWSServiceRoleForSecurityHubV2` Bei dieser dienstverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Security Hub verknüpft ist. Sie wird von Security Hub vordefiniert und beinhaltet alle Berechtigungen, die Security Hub benötigt, um andere AWS Ressourcen in Ihrem Namen anzurufen AWS-Services und zu überwachen. Security Hub verwendet diese dienstbezogene Rolle überall dort, AWS-Regionen wo Security Hub verfügbar ist.

Eine dienstgebundene Rolle erleichtert die Einrichtung von Security Hub, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Security Hub definiert die Berechtigungen seiner dienstverknüpften Rolle. Sofern nicht anders definiert, kann nur Security Hub die Rolle übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und Sie können diese Berechtigungsrichtlinie keiner anderen IAM-Entität zuordnen.

Um die Details der dienstverknüpften Rolle zu überprüfen, können Sie die Security Hub-Konsole verwenden. Wählen Sie im Navigationsbereich unter Einstellungen die Option Allgemein aus. Wählen Sie dann im Abschnitt Serviceberechtigungen die Option Dienstberechtigungen anzeigen aus.

Sie können die dienstgebundene Security Hub-Rolle erst löschen, nachdem Sie Security Hub in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dies schützt Ihre Security Hub-Ressourcen, da Sie nicht versehentlich Zugriffsberechtigungen entfernen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Rollen nach den Diensten, für die Ja steht. Service-linked Wählen Sie Ja mit einem Link aus, um die Dokumentation zur dienstverknüpften Rolle für diesen Dienst zu überprüfen.

Themen

- Service-linked Rollenberechtigungen für Security Hub
- Erstellen einer dienstverknüpften Rolle für Security Hub

- Bearbeitung einer dienstverknüpften Rolle für Security Hub
- Löschen einer dienstverknüpften Rolle für Security Hub

Service-linked Rollenberechtigungen für Security Hub

Security Hub verwendet die dienstverknüpfte Rolle namens`AWSServiceRoleForSecurityHubV2`. Es handelt sich um eine dienstbezogene Rolle, die AWS Security Hub benötigt, um auf Ihre Ressourcen zuzugreifen. Diese dienstbezogene Rolle ermöglicht es Security Hub, Aufgaben wie das Empfangen von Ergebnissen von anderen Benutzern AWS-Services und das Konfigurieren der erforderlichen AWS Config Infrastruktur für die Durchführung von Sicherheitsprüfungen für Kontrollen auszuführen. Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHubV2` vertraut dem Service `securityhub.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHubV2` verwendet die verwaltete Richtlinie `AWSSecurityHubV2ServiceRolePolicy`.

Sie müssen einer IAM-Identität (z. B. einer Rolle, Gruppe oder einem Benutzer) Berechtigungen gewähren, um eine serviceverknüpfte Rolle zu erstellen, zu bearbeiten oder zu löschen. Damit die `AWSServiceRoleForSecurityHubV2` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie für den Zugriff auf Security Hub verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Identität an.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Erstellen einer dienstverknüpften Rolle für Security Hub

Die `AWSServiceRoleForSecurityHubV2` serviceverknüpfte Rolle wird automatisch erstellt, wenn Sie Security Hub zum ersten Mal aktivieren oder wenn Sie Security Hub in einer Region aktivieren, in der Sie sie zuvor nicht aktiviert haben. Sie können die `AWSServiceRoleForSecurityHubV2` serviceverknüpfte Rolle auch manuell mithilfe der IAM-Konsole, der IAM-CLI oder der IAM-API erstellen. Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

> **Important**
>
> Die dienstgebundene Rolle, die für ein Security Hub-Administratorkonto erstellt wird, gilt nicht für zugehörige Security Hub-Mitgliedskonten.

Bearbeitung einer dienstverknüpften Rolle für Security Hub

Security Hub ermöglicht es Ihnen nicht, die `AWSServiceRoleForSecurityHubV2` dienstverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstverknüpften Rolle für Security Hub

Wenn Sie eine Funktion oder einen Dienst, für den eine dienstbezogene Rolle erforderlich ist, nicht mehr benötigen, löschen Sie die Rolle. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

Wenn Sie Security Hub deaktivieren, löscht Security Hub die mit dem `AWSServiceRoleForSecurityHubV2` Dienst verknüpfte Rolle nicht automatisch für Sie. Wenn Sie Security Hub erneut aktivieren, kann der Dienst dann wieder die vorhandene dienstverknüpfte Rolle

verwenden. Wenn Sie Security Hub nicht mehr verwenden müssen, können Sie die dienstverknüpfte Rolle manuell löschen.

> **Important**
>
> Bevor Sie die `AWSServiceRoleForSecurityHubV2` dienstverknüpfte Rolle löschen, müssen Sie Security Hub zunächst in allen Regionen deaktivieren, in denen sie aktiviert ist. Weitere Informationen finden Sie unter Security Hub deaktivieren. Wenn Security Hub nicht deaktiviert ist, wenn Sie versuchen, die serviceverknüpfte Rolle zu löschen, schlägt das Löschen fehl.

Um die `AWSServiceRoleForSecurityHubV2` serviceverknüpfte Rolle zu löschen, können Sie die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

AWSverwaltete Richtlinien für Security Hub

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wirdAWS. AWSVerwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWSverwaltete Richtlinie: AWSSecurityHubFullAccess

Sie können die `AWSSecurityHubFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Security Hub Hub-Aktionen gewähren. Diese Richtlinie muss einem Prinzipal zugewiesen werden, bevor er Security Hub manuell für sein Konto aktiviert. Principals mit diesen Berechtigungen können beispielsweise den Status der Ergebnisse sowohl einsehen als auch aktualisieren. Sie können auch benutzerdefinierte Einblicke konfigurieren, Integrationen aktivieren sowie Standards und Kontrollen aktivieren und deaktivieren. Principals für ein Administratorkonto können auch Mitgliedskonten verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `securityhub`— Ermöglicht Prinzipalen vollen Zugriff auf alle Security Hub Hub-Aktionen.
- `guardduty`— Ermöglicht Principals, Informationen über den Kontostatus bei Amazon GuardDuty abzurufen.
- `iam`— Ermöglicht Prinzipalen, eine dienstbezogene Rolle für Security Hub zu erstellen.
- `inspector`— Ermöglicht Principals, Informationen zum Kontostatus in Amazon Inspector abzurufen.
- `pricing`— Ermöglicht Principals, eine Preisliste mit Produkten zu erhalten. AWS-Services

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWSverwaltete Richtlinie: AWSSecurityHubReadOnlyAccess

Sie können die `AWSSecurityHubReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in Security Hub einzusehen. Principals, denen diese Richtlinie beigefügt ist, können keine Updates in Security Hub vornehmen. Principals mit diesen Berechtigungen können beispielsweise die mit ihrem Konto verknüpfte Ergebnisliste einsehen, den Status eines Fundes jedoch nicht ändern. Sie können die Ergebnisse von Insights einsehen, aber keine benutzerdefinierten Insights erstellen oder konfigurieren. Sie können keine Steuerungen oder Produktintegrationen konfigurieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `securityhub`— Ermöglicht Benutzern das Ausführen von Aktionen, bei denen eine Liste von Artikeln oder Details zu einem Artikel zurückgegeben wird. Dazu gehören API-Operationen, die mit `GetList`, oder beginnen`Describe`.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubReadOnlyAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWSverwaltete Richtlinie: AWSSecurityHubOrganizationsAccess

Sie können die `AWSSecurityHubOrganizationsAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen zur Aktivierung und Verwaltung von Security Hub für eine Organisation inAWS Organizations. Die Berechtigungen für diese Richtlinie ermöglichen es dem Organisationsverwaltungskonto, das delegierte Administratorkonto für Security Hub festzulegen. Sie ermöglichen es dem delegierten Administratorkonto auch, Organisationskonten als Mitgliedskonten zu aktivieren.

Diese Richtlinie bietet nur Berechtigungen fürAWS Organizations. Das Organisationsverwaltungskonto und das delegierte Administratorkonto erfordern ebenfalls Berechtigungen für zugehörige Aktionen. Diese Berechtigungen können mithilfe der `AWSSecurityHubFullAccess` verwalteten Richtlinie erteilt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `organizations:ListAccounts`— Ermöglicht Prinzipalen das Abrufen der Liste der Konten, die Teil einer Organisation sind.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisation.
- `organizations:ListRoots`— Ermöglicht Prinzipalen, das Stammverzeichnis einer Organisation aufzulisten.
- `organizations:ListDelegatedAdministrators`— Ermöglicht Prinzipalen, den delegierten Administrator einer Organisation aufzulisten.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Prinzipalen, diejenigen aufzulistenAWS-Services, die eine Organisation verwendet.

- `organizations:ListOrganizationalUnitsForParent`— Ermöglicht Prinzipalen, die untergeordneten Organisationseinheiten (OU) einer übergeordneten OU aufzulisten.
- `organizations:ListAccountsForParent`— Ermöglicht Prinzipalen, die untergeordneten Konten einer übergeordneten Organisationseinheit aufzulisten.
- `organizations:ListParents`— Führt die Stamm- oder Organisationseinheiten (OUs) auf, die der angegebenen untergeordneten Organisationseinheit oder dem angegebenen untergeordneten Konto als unmittelbare übergeordnete Einheit dienen.
- `organizations:DescribeAccount` – Ermöglicht Prinzipalen den Abruf von Informationen über ein Konto in der Organisation.
- `organizations:DescribeOrganizationalUnit`— Ermöglicht Prinzipalen das Abrufen von Informationen über eine Organisationseinheit in der Organisation.
- `organizations:ListPolicies`— Ruft die Liste aller Richtlinien in einer Organisation eines bestimmten Typs ab.
- `organizations:ListPoliciesForTarget`— Führt die Richtlinien auf, die direkt mit dem angegebenen Zielstamm, der Organisationseinheit (OU) oder dem angegebenen Konto verknüpft sind.
- `organizations:ListTargetsForPolicy`— Führt alle Stammverzeichnisse, Organisationseinheiten (OUs) und Konten auf, denen die angegebene Richtlinie zugeordnet ist.
- `organizations:EnableAWSServiceAccess`— Ermöglicht Prinzipalen, die Integration mit Organizations zu ermöglichen.
- `organizations:RegisterDelegatedAdministrator`— Ermöglicht es den Prinzipalen, das delegierte Administratorkonto festzulegen.
- `organizations:DeregisterDelegatedAdministrator`— Ermöglicht Prinzipalen, das delegierte Administratorkonto zu entfernen.
- `organizations:DescribePolicy`— Ruft Informationen zu einer Richtlinie ab.
- `organizations:DescribeEffectivePolicy`— Gibt den Inhalt der gültigen Richtlinie für den angegebenen Richtlinientyp und das angegebene Konto zurück.
- `organizations:CreatePolicy`— Erstellt eine Richtlinie eines bestimmten Typs, die Sie einem Stammkonto, einer Organisationseinheit (OU) oder einem einzelnen AWS Konto zuordnen können.
- `organizations:UpdatePolicy`— Aktualisiert eine bestehende Richtlinie mit einem neuen Namen, einer neuen Beschreibung oder einem neuen Inhalt.
- `organizations:DeletePolicy`— Löscht die angegebene Richtlinie aus Ihrer Organisation.

- `organizations:AttachPolicy`— Fügt eine Richtlinie einem Stammkonto, einer Organisationseinheit (OU) oder einem Einzelkonto hinzu.
- `organizations:DetachPolicy`— Trennt eine Richtlinie von einem Zielstamm, einer Organisationseinheit (OU) oder einem Zielkonto.
- `organizations:EnablePolicyType`— Aktiviert einen Richtlinientyp in einem Stamm.
- `organizations:DisablePolicyType`— Deaktiviert einen Organisationsrichtlinientyp in einem Stamm.
- `organizations:TagResource`— Fügt einer angegebenen Ressource ein oder mehrere Tags hinzu.
- `organizations:UntagResource`— Entfernt alle Tags mit den angegebenen Schlüsseln aus einer angegebenen Ressource.
- `organizations:ListTagsForResource`— Listet Tags auf, die an eine angegebene Ressource angehängt sind.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubOrganizationsAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWSverwaltete Richtlinie: AWSSecurityHubV2ServiceRolePolicy

Diese Richtlinie ermöglicht es Security Hub, AWS Config Regeln und Security Hub Hub-Ressourcen für Ihre Organisation und in Ihrem Namen zu verwalten. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre IAM-Identitäten anfügen. Weitere Informationen finden Sie unter the section called “Service-linked Rollen”.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `access-analyzer`— Erstellen und löschen Sie serviceverknüpfte IAM Access Analyzer, wenn Kunden Security Hub aktivieren oder deaktivieren, listen Sie Analyzer auf, um zu überprüfen, ob der Status des Analyzers mit dem Aktivierungsstatus übereinstimmt, und generieren und rufen Sie Richtlinienempfehlungen für ungenutzte Zugriffsergebnisse ab.
- `cloudwatch`— Rufen Sie Metrikdaten ab, um Messfunktionen für Security Hub Hub-Ressourcen und Connector-Integritätsmetriken zu unterstützen.
- `config`— Verwaltung von serviceverknüpften Konfigurationsrekordern und serviceverknüpften Konfigurationsrekordern von Drittanbietern für Security Hub Hub-Ressourcen, einschließlich

Unterstützung für globale Config-Recorder. Listet Konfigurationsrekorder auf und ruft Konnektorinformationen zur Unterstützung von Cloud-Integrationen von Drittanbietern ab.

- `ecr`— Rufen Sie Informationen über Amazon Elastic Container Registry-Images und Repositorys ab, um Messfunktionen zu unterstützen.
- `iam`— Erstellen Sie die folgenden serviceverknüpften Rollen:AWS Config, IAM Access Analyzer im Kundenkonto und Amazon Inspector für Drittanbieter-Scans. Rufen Sie Kontoinformationen ab, um die Messfunktionen zu unterstützen. Rufen Sie bestehende IAM-Richtlinien ab, sodass Kunden einen Vergleich ihrer aktuellen Richtlinie und der empfohlenen Alternative mit den geringsten Rechten einsehen können.
- `inspector2`— Amazon Inspector Inspector-Konnektoren und Connector-Scan-Konfigurationen erstellen, aktualisieren, löschen und auflisten, um Cloud-Integrationen von Drittanbietern zu unterstützen.
- `lambda`— Rufen Sie AWS Lambda Funktionsinformationen ab, um Messfunktionen zu unterstützen.
- `organizations`— Rufen Sie Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.
- `securityhub`— Verwaltet die Security Hub Hub-Konfiguration. Erstellen, aktualisieren und löschen Sie Security Hub Hub-Connectors, um Cloud-Integrationen von Drittanbietern zu unterstützen.
- `sts`— Besorgen Sie sich Web-Identitätstoken für den ausgehenden Identitätsverbund zur Unterstützung von Cloud-Integrationen von Drittanbietern.
- `tag`— Rufen Sie Informationen zu Ressourcen-Tags ab.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubV2ServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Security Hub Hub-Updates fürAWSVerwaltete Richtlinien

Die folgende Tabelle enthält Einzelheiten zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Security Hub, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Security Hub Hub-Dokumentverlaufsseite, um automatische Benachrichtigungen über Aktualisierungen der Richtlinien zu erhalten.

Änderungen	Beschreibung	Date
AWSSecurityHubV2ServiceRolePolicy – Richtlinie aktualisieren	Security Hub hat die Richtlinie aktualisiert, um Integrationen von Drittanbietern zu unterstützen. Das Update fügt die folgenden Berechtigungen hinzu: Konfigurationsrekorder von Drittanbietern verwalten, Security Hub- und Amazon Inspector-Connectors erstellen und verwalten, Connector-Integritätsmetriken von CloudWatch abrufen, die mit dem Amazon Inspector-Service verknüpfte Rolle für Drittanbieter-Scans erstellen und Web-Identitätstoken für den Verbund abrufen.	30. Juni 2026
AWSSecurityHubV2ServiceRolePolicy – Richtlinie aktualisieren	Security Hub hat die Richtlinie aktualisiert, um IAM Access Analyzer-Berechtigungen hinzuzufügen. Das Update ermöglicht es Security Hub, service-verwaltete Analyzer zu erstellen und zu verwalten, Analyzer aufzulisten, um zu überprüfen, ob die Analyzer-Konfiguration dem Aktivierungsstatus entspricht, Richtlinienempfehlungen für ungenutzte Zugriffsergebnisse zu generieren und abzurufen und IAM-Richtlinien für die Anzeige von Empfehlungen abzurufen.	10. Mai 2026

Änderungen	Beschreibung	Date
AWSSecurityHubOrganizationsAccess – Richtlinie aktualisieren	Security Hub hat die Richtlinie aktualisiert, um Berechtigungen zur Beschreibung von Ressourcenrichtlinien zur Unterstützung von Security Hub Hub-Funktionen hinzuzufügen. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	12. November 2025
AWSSecurityHubFullAccess – Richtlinie aktualisieren	Security Hub hat die Richtlinie aktualisiert und Funktionen zur Verwaltung GuardDuty, Amazon Inspector und Kontoverwaltung hinzugefügt, um die Funktionen von Security Hub zu unterstützen. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	17. November 2025

Änderungen	Beschreibung	Date
AWSSecurityHubV2ServiceRolePolicy – Richtlinie aktualisieren	Security Hub hat die Richtlinie aktualisiert, um Messfunktionen für Amazon Elastic Container Registry und Amazon CloudWatch hinzuzufügen und Security Hub Hub-Funktionen AWS Identity and Access Management zu unterstützen. AWS Lambda Das Update fügte auch Unterstützung für globale AWS Config Rekorder hinzu. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	5. November 2025
AWSSecurityHubOrganizationsAccess – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat der Richtlinie neue Berechtigungen hinzugefügt. Die Berechtigungen ermöglichen es der Organisationsleitung, Security Hub und Security Hub CSPM für eine Organisation zu aktivieren und zu verwalten.	17. Juni 2025
AWSSecurityHubFullAccess – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, eine dienstbezogene Rolle für Security Hub zu erstellen.	17. Juni 2025

Änderungen	Beschreibung	Date
AWSSecurityHubV2ServiceRolePolicy – Neue Richtlinie	Security Hub hat eine neue Richtlinie hinzugefügt, die es Security Hub ermöglicht, AWS Config Regeln und Security Hub Hub-Ressourcen für die Organisation eines Kunden und im Namen des Kunden zu verwalten. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	17. Juni 2025
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um Preisdetails für AWS-Services und Produkte zu erhalten.	24. April 2024
AWSSecurityHubReadOnlyAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat diese verwaltete Richtlinie aktualisiert, indem ein `Sid` Feld hinzugefügt wurde.	22. Februar 2024
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, sodass festgestellt werden kann, ob Amazon GuardDuty und Amazon Inspector in einem Konto aktiviert sind. Dies hilft Kunden dabei, sicherheitsrelevante Informationen aus mehreren AWS-Services zusammenzuführen.	16. November 2023

Änderungen	Beschreibung	Date
AWSSecurityHubOrganizationsAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um zusätzliche Berechtigungen für den schreibgeschützten Zugriff auf delegierte Administratorfunktionen zu AWS Organizations gewähren. Dazu gehören Details wie das Stammverzeichnis, die Organisationseinheiten (OUs), die Konten, die Organisationsstruktur und der Servicezugriff.	16. November 2023
AWSSecurityHubOrganizationsAccess— Neue Richtlinie	Security Hub CSPM hat eine neue Richtlinie hinzugefügt, die Berechtigungen gewährt, die für die Security Hub CSPM-Integration mit Organizations erforderlich sind.	15. März 2021
Security Hub CSPM hat begonnen, Änderungen zu verfolgen	Security Hub CSPM begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	15. März 2021

Fehlerbehebung AWS Identität und Zugriff auf den Security Hub

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Security Hub und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Security Hub auszuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole

- Ich möchte programmatischen Zugriff auf Security Hub erhalten
- Ich bin Administrator und möchte anderen den Zugriff auf Security Hub ermöglichen
- Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Security Hub-Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Security Hub auszuführen

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie Ihren Administrator um Unterstützung bitten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einem anzuzeigen, *`widget`* aber nicht über die `securityhub:`*`GetWidget`* erforderlichen Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `securityhub:`*`GetWidget`* zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Security Hub übergeben können.

In einigen Fällen AWS-Services können Sie eine vorhandene Rolle an diesen Dienst übergeben, anstatt eine neue oder mit dem Dienst verknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Security Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte programmatischen Zugriff auf Security Hub erhalten

Benutzer benötigen programmgesteuerten Zugriff, wenn sie AWS außerhalb von interagieren möchten. AWS-Managementkonsole Die Art und Weise, wie programmgesteuerter Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldedaten als temporäre Anmeldeinformationen, um programmatische Anforderungen an die AWS SDKs AWS CLI oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie im AWS Command Line Interface Benutzerhandbuch unter Anmeldung für AWS lokale Entwicklung. AWS CLI • Informationen zu AWS SDKs finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch für AWS SDKs und Tools.
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS SDKs oder AWS CLI APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		• Informationen dazu finden Sie AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch unter Configuring AWS CLI to use. AWS CLI • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS SDKs oder APIs AWS CLI zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie im AWS CLI Benutzerhandbuch unter Authentifizierung mit IAM-Benutzeranmeldeinformationen. AWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen den Zugriff auf Security Hub ermöglichen

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Security Hub-Ressourcen zuzugreifen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Security Hub diese Funktionen unterstützt, finden Sie unterSo funktioniert Security Hub mit IAM.
- Informationen zum Bereitstellen des Zugriffs auf Ihre Ressourcen in Ihrem eigenen AWS-Konten Bereich finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dessen Eigentümer Sie sind.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf Ressourcen, die Dritten AWS-Konten gehören.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsüberprüfung für AWS Sicherheitszentrum

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen für AWS Ihre Umgebung anmelden oder diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme, .

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen im Abschnitt Berichte AWS Artifact .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz in AWS Sicherheitszentrum

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS Sicherheitszentrum

Als verwalteter Dienst ist AWS Security Hub durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung anhand der Best Practices für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Security Hub zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungssammlungen mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

AWS Security Hub und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Security Hub herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Security Hub-APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN- oder AWS Direct Connect-Verbindung erforderlich ist. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Security Hub-APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Security Hub verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen finden Sie im Amazon Virtual Private Cloud-Handbuch unter Zugreifen auf und AWS-Service mithilfe eines VPC-Schnittstellen-Endpunkts.

Überlegungen zu Security Hub-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Security Hub einrichten, stellen Sie sicher, dass Sie die Voraussetzungen und andere Informationen im Amazon Virtual Private Cloud-Handbuch lesen.

Security Hub unterstützt das Aufrufen aller seiner API-Aktionen von Ihrer VPC aus.

Erstellen eines VPC-Schnittstellen-Endpunkts für Security Hub

Sie können einen VPC-Endpunkt für den Security Hub-Service entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im Amazon Virtual Private Cloud-Handbuch.

Erstellen Sie einen VPC-Endpunkt für Security Hub mit dem folgenden Servicenamen:

```
com.amazonaws.region.securityhub
```

Wo *region* ist der Regionalcode für den AWS-Region zutreffenden.

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Security Hub unter Verwendung des Standard-DNS-Namens für die Region stellen, z. B. `securityhub.us-east-1.amazonaws.com` für die Region USA Ost (Nord-Virginia).

Erstellen einer VPC-Endpunktrichtlinie für Security Hub

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Security Hub steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon Virtual Private Cloud Guide.

Beispiel: VPC-Endpunktrichtlinie für Security Hub-Aktionen

Das Folgende ist ein Beispiel für eine Endpunktrichtlinie für Security Hub. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Security Hub-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Gemeinsam genutzte Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen gemeinsam genutzt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden. Informationen zur VPC-Freigabe finden Sie im Amazon Virtual Private Cloud-Handbuch unter Teilen Sie Ihre VPC-Subnetze mit anderen Konten.

Protokollierung von Security Hub-API-Aufrufen mit CloudTrail

ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Security Hub bereitstellt. CloudTrail erfasst API-Aufrufe für Security Hub als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Hub-Konsole und Codeaufrufe an die Security Hub-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Security Hub. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der CloudTrail gesammelten Informationen können Sie ermitteln, welche Anfrage an Security Hub gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum Security Hub finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Security Hub eine unterstützte Ereignisaktivität auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Eventverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem Konto, einschließlich der Ereignisse für Security Hub, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere AWS Dienste so konfigurieren, dass sie die in den CloudTrail Protokollen

gesammelten Ereignisdaten weiter analysieren und darauf reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Security Hub unterstützt die Protokollierung aller Security Hub-API-Aktionen als Ereignisse in CloudTrail Protokollen. Eine Liste der Security Hub-Operationen finden Sie in der Security Hub-API-Referenz.

Wenn die Aktivität für die folgenden Aktionen protokolliert wird CloudTrail, `responseElements` wird der Wert für auf gesetzt`null`. Dadurch wird sichergestellt, dass vertrauliche Informationen nicht in CloudTrail Protokollen enthalten sind.

- `GetFindingsV2`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Beispiel: Einträge in der Security Hub-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der

Aktion, Anforderungsparameter usw. CloudTrail Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Logeintrag, der die `CreateAutomationRuleV2` Aktion demonstriert. In diesem Beispiel `TestAutomationRule` wird eine Automatisierungsregel mit dem Namen erstellt. Die `Account ID` Attribute `Severity` und werden als Kriterien angegeben. Wenn die Regel erfüllt ist, `Severity` wird die auf Hoch aktualisiert. Weitere Informationen zu Automatisierungsregeln finden Sie unterAutomatisierungsregeln in Security Hub.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:Admin",
        "arn": "arn:aws:sts::555555555555:assumed-role/Admin",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "aarn:aws:iam::555555555555:role/Admin",
                "accountId": "555555555555",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2025-11-15T18:49:13Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-11-15T18:51:17Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateAutomationRuleV2",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.50",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Description": "Test Automation Rule",
        "Actions": [
            {
                "Type": "FINDING_FIELDS_UPDATE",
                "FindingFieldsUpdate": {
```

```
                    "SeverityId": 4
                }
            }
        ],
        "RuleStatus": "ENABLED",
        "Criteria": {
            "OcsfFindingCriteria": {
                "CompositeFilters": [
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "severity",
                                "Filter": {
                                    "Value": "Medium",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    },
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "cloud.account.uid",
                                "Filter": {
                                    "Value": "111122223333",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    }
                ],
                "CompositeOperator": "AND"
            }
        },
        "ClientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
        "RuleOrder": 61,
        "RuleName": "TestAutomationRule",
        "Tags": {}
    },
    "responseElements": {
        "RuleArn": "arn:aws:securityhub:us-west-2:555555555555:automation-rulev2/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
        "RuleId": "c8bc6f90-29e9-4eb7-919f-b145e44eb8ec"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management"
}
```

Einführung in AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices zu bewerten.

AWS Security Hub CSPM sammelt Sicherheitsdaten für und unterstützte Produkte von Drittanbietern und hilft Ihnen dabei AWS-Konten AWS-Services, Ihre Sicherheitstrends zu analysieren und Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Um Ihnen bei der Verwaltung des Sicherheitsstatus Ihres Unternehmens zu helfen, unterstützt Security Hub CSPM mehrere Sicherheitsstandards. Dazu gehören der vom Center for Internet Security (CIS) entwickelte AWS Standard AWS Foundational Security Best Practices (FSBP) und externe Compliance-Frameworks wie das Center for Internet Security (CIS), der Payment Card Industry Data Security Standard (PCI DSS) und das National Institute of Standards and Technology (NIST). Jeder Standard umfasst mehrere Sicherheitskontrollen, von denen jede eine bewährte Sicherheitsmethode darstellt. Security Hub CSPM führt Prüfungen anhand von Sicherheitskontrollen durch und generiert Kontrollergebnisse, anhand derer Sie Ihre Einhaltung anhand bewährter Sicherheitsverfahren beurteilen können.

Security Hub CSPM generiert nicht nur Kontrollergebnisse, sondern erhält auch Ergebnisse von anderen Produkten AWS-Services— wie Amazon GuardDuty, Amazon Inspector und Amazon Macie — und von unterstützten Produkten von Drittanbietern. Auf diese Weise erhalten Sie einen zentralen Überblick über eine Vielzahl von sicherheitsrelevanten Problemen. Sie können die Ergebnisse des Security Hub CSPM auch an andere AWS-Services und unterstützte Produkte von Drittanbietern senden.

Security Hub CSPM bietet Automatisierungsfunktionen, mit denen Sie Sicherheitsprobleme erkennen und beheben können. Beispielsweise können Sie Automatisierungsregeln verwenden, um wichtige Ergebnisse automatisch zu aktualisieren, wenn eine Sicherheitsüberprüfung fehlschlägt. Sie können die Integration mit Amazon auch nutzen EventBridge , um automatische Antworten auf bestimmte Ergebnisse auszulösen.

Themen

- Vorteile von Security Hub CSPM
- Zugreifen auf Security Hub CSPM
- Zugehörige Services

- Kostenlose Testversion von Security Hub CSPM und Preisgestaltung
- Konzepte und Terminologie in Security Hub CSPM
- Security Hub CSPM aktivieren
- Verwaltung von Administrator- und Mitgliedskonten in Security Hub CSPM
- Grundlegendes zur regionsübergreifenden Aggregation in Security Hub CSPM
- Sicherheitsstandards in Security Hub CSPM verstehen
- Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM
- Integrationen in Security Hub CSPM verstehen
- Integration von Security Hub CSPM mit Microsoft Azure
- Ergebnisse in Security Hub CSPM erstellen und aktualisieren
- Einblicke in Security Hub CSPM anzeigen
- Ergebnisse in Security Hub CSPM automatisch ändern und darauf reagieren
- Arbeiten mit dem Dashboard in Security Hub CSPM
- Regionale Grenzwerte für Security Hub CSPM
- Security Hub CSPM-Ressourcen erstellen mit CloudFormation
- Abonnieren von Security Hub CSPM-Ankündigungen mit Amazon SNS
- Security Hub CSPM deaktivieren
- Sicherheit bei AWS Security Hub CSPM
- Security Hub Hub-API-Aufrufe protokollieren mit CloudTrail

Vorteile von Security Hub CSPM

Im Folgenden sind einige der wichtigsten Methoden aufgeführt, mit denen Security Hub CSPM Sie bei der Überwachung Ihrer Compliance- und Sicherheitslage in Ihrer AWS gesamten Umgebung unterstützt.

Reduzierter Aufwand zur Erfassung und Priorisierung von Ergebnissen

Security Hub CSPM reduziert den Aufwand für die Erfassung und Priorisierung von Sicherheitsergebnissen für alle Konten aus integrierten Produkten AWS-Services und AWS Partnerprodukten. Security Hub CSPM verarbeitet Suchdaten mit dem AWS Security Finding Format (ASFF), einem Standardsuchformat. Dadurch entfällt die Notwendigkeit, Ergebnisse aus

unzähligen Quellen in verschiedenen Formaten zu verwalten. Security Hub CSPM korreliert die Ergebnisse auch anbieterübergreifend, um Ihnen zu helfen, die wichtigsten zu priorisieren.

Automatische Sicherheitsprüfungen nach bewährten Methoden und Standards

Security Hub CSPM führt automatisch kontinuierliche Konfigurationen und Sicherheitsprüfungen auf Kontoebene durch, die auf AWS Best Practices und Industriestandards basieren. Security Hub CSPM berechnet anhand der Ergebnisse dieser Prüfungen Sicherheitsbewertungen und identifiziert bestimmte Konten und Ressourcen, die besondere Aufmerksamkeit erfordern.

Konsolidierte Ansicht der Ergebnisse über Konten und Anbieter hinweg

Security Hub CSPM konsolidiert Ihre Sicherheitsergebnisse für Konten und Anbieterprodukte und zeigt die Ergebnisse auf der Security Hub CSPM-Konsole an. Sie können Ergebnisse auch über die Security Hub CSPM-API oder SDKs abrufen. AWS CLI Mit einem ganzheitlichen Überblick über Ihren aktuellen Sicherheitsstatus können Sie Trends erkennen, potenzielle Probleme identifizieren und die erforderlichen Abhilfemaßnahmen ergreifen.

Fähigkeit, die Suche nach Updates und Problembehebungen zu automatisieren

Sie können Automatisierungsregeln erstellen, mit denen Ergebnisse auf der Grundlage Ihrer definierten Kriterien geändert oder unterdrückt werden. Security Hub CSPM unterstützt auch eine Integration mit Amazon. EventBridge Um die Behebung bestimmter Ergebnisse zu automatisieren, können Sie benutzerdefinierte Aktionen definieren, die ergriffen werden, wenn ein Ergebnis generiert wird. Sie können beispielsweise benutzerdefinierte Aktionen konfigurieren, damit Ergebnisse an ein Ticketing-System oder ein automatisiertes Behebungssystem gesendet werden.

Zugreifen auf Security Hub CSPM

Security Hub CSPM ist in den meisten Fällen verfügbar. AWS-Regionen Eine Liste der Regionen, in denen Security Hub CSPM derzeit verfügbar ist, finden Sie unter AWS Security Hub CSPM-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz Informationen zur Verwaltung AWS-Regionen für Sie finden Sie im AWS-Konto Referenzhandbuch unter Spezifizieren, welche AWS-Regionen Ihr Konto verwenden kann.AWS -Kontenverwaltung

In jeder Region können Sie auf eine der folgenden Arten auf Security Hub CSPM zugreifen und es verwenden:

Security Hub CSPM-Konsole

Das AWS-Managementkonsole ist eine browserbasierte Oberfläche, mit der Sie Ressourcen erstellen und verwalten können. AWS Als Teil dieser Konsole bietet die Security Hub CSPM-Konsole Zugriff auf Ihr Security Hub CSPM-Konto, Ihre Daten und Ressourcen. Sie können Security Hub CSPM-Aufgaben mithilfe der Security Hub CSPM-Konsole ausführen — Ergebnisse anzeigen, Automatisierungsregeln erstellen, eine Aggregationsregion erstellen und vieles mehr.

Security Hub CSPM API

Die Security Hub CSPM-API ermöglicht Ihnen programmatischen Zugriff auf Ihr Security Hub CSPM-Konto, Ihre Daten und Ressourcen. Mit der API können Sie HTTPS-Anfragen direkt an Security Hub CSPM senden. Informationen zur API finden Sie in der AWS Security Hub API-Referenz.

AWS CLI

Mit dem AWS CLI können Sie Befehle an der Befehlszeile Ihres Systems ausführen, um Security Hub CSPM-Aufgaben auszuführen. In einigen Fällen kann die Verwendung der Befehlszeile schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeile ist auch nützlich, wenn Sie Skripts erstellen möchten, die Aufgaben ausführen. Informationen zur Installation und Verwendung von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen, z. B. Java, Go, Python, C++ und .NET. Die SDKs bieten bequemen, programmatischen Zugriff auf Security Hub CSPM und andere Programme AWS-Services in Ihrer bevorzugten Sprache. Sie erledigen auch Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter Tools to Build On. AWS

Important

Security Hub CSPM erkennt und konsolidiert nur Ergebnisse, die nach der Aktivierung von Security Hub CSPM generiert wurden. Sicherheitsergebnisse, die vor der Aktivierung von Security Hub CSPM generiert wurden, werden nicht rückwirkend erkannt und konsolidiert. Security Hub CSPM empfängt und verarbeitet Ergebnisse nur in der Region, in der Sie Security Hub CSPM in Ihrem Konto aktiviert haben.

Um die vollständige Einhaltung der Benchmark-Sicherheitsprüfungen der CIS AWS Foundations zu gewährleisten, müssen Sie Security Hub CSPM in allen unterstützten AWS Regionen aktivieren.

Zugehörige Services

Um Ihre AWS Umgebung weiter zu schützen, sollten Sie die Verwendung von Other AWS-Services in Kombination mit Security Hub CSPM in Betracht ziehen. Einige AWS-Services senden ihre Ergebnisse an Security Hub CSPM, und Security Hub CSPM normalisiert die Ergebnisse in ein Standardformat. Einige AWS-Services können auch Ergebnisse von Security Hub CSPM erhalten.

Eine Liste anderer Benutzer AWS-Services , die Security Hub CSPM-Ergebnisse senden oder empfangen, finden Sie unter. AWS-Service Integrationen mit Security Hub CSPM

Security Hub CSPM verwendet dienstbezogene Regeln von, AWS Config um Sicherheitsüberprüfungen für die meisten Kontrollen durchzuführen. Kontrollen beziehen sich auf bestimmte AWS-Services Ressourcen. AWS Eine Liste der Security Hub CSPM-Steuerelemente finden Sie unter. Kontrollreferenz für Security Hub CSPM Sie müssen Ressourcen AWS Config für Security Hub CSPM aktivieren AWS Config und aufzeichnen, um die meisten Kontrollergebnisse zu generieren. Weitere Informationen finden Sie unter Überlegungen vor der Aktivierung und Konfiguration AWS Config.

Kostenlose Testversion von Security Hub CSPM und Preisgestaltung

Wenn Sie Security Hub CSPM zum ersten Mal aktivieren, wird dieses Konto automatisch AWS-Konto für eine kostenlose 30-Tage-Testversion von Security Hub CSPM registriert.

Wenn Sie Security Hub CSPM während der kostenlosen Testversion verwenden, wird Ihnen die Nutzung anderer Dienste, mit denen Security Hub CSPM interagiert, wie z. B. Artikel, in Rechnung gestellt. AWS Config AWS Config Regeln, die nur durch die Security Hub CSPM-Sicherheitsstandards aktiviert werden, werden Ihnen nicht in Rechnung gestellt.

Die Nutzung von Security Hub CSPM wird Ihnen erst nach Ablauf Ihrer kostenlosen Testversion in Rechnung gestellt.

Nutzungsdetails anzeigen

Security Hub CSPM stellt Nutzungsinformationen bereit, einschließlich der Anzahl der von Ihrem Konto verarbeiteten Sicherheitsprüfungen und Ergebnisse. Die Nutzungsdetails beinhalten auch die verbleibende Zeit der kostenlosen Testversion. Diese Informationen können Ihnen helfen, Ihre Security Hub CSPM-Nutzung nach Ablauf der kostenlosen Testversion zu verstehen. Die Nutzungsinformationen sind auch nach Ablauf der kostenlosen Testversion verfügbar.

Um Nutzungsinformationen anzuzeigen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Verwendung aus.

Die Nutzungsinformationen beziehen sich nur auf das aktuelle Konto und die aktuelle Region. In einer Aggregationsregion enthalten die Nutzungsinformationen keine verknüpften Regionen. Weitere Informationen zu verknüpften Regionen finden Sie unterthe section called “Arten von Daten, die aggregiert sind”.

Um die Kostendetails für Ihr Konto einzusehen, verwenden Sie die AWS Abrechnungskonsole.

Preisdetails

Weitere Informationen darüber, wie Security Hub CSPM für aufgenommene Ergebnisse und Sicherheitsprüfungen Gebühren erhebt, finden Sie unter Security Hub CSPM — Preise.

Konzepte und Terminologie in Security Hub CSPM

In AWS Security Hub CSPM bauen wir auf gemeinsamen AWS Konzepten und Terminologie auf und verwenden diese zusätzlichen Begriffe.

Account

Ein Standardkonto bei Amazon Web Services (AWS), das Ihre AWS Ressourcen enthält. Sie können sich AWS mit Ihrem Konto anmelden und Security Hub CSPM aktivieren.

Ein Konto kann andere Konten zur Aktivierung von Security Hub CSPM einladen und diesem Konto in Security Hub CSPM zugeordnet werden. Das Annehmen einer Mitgliedschaftseinladung ist optional. Wenn die Einladungen akzeptiert werden, wird das

Konto zu einem Administratorkonto und die hinzugefügten Konten sind Mitgliedskonten. Administratorkonten können Ergebnisse in ihren Mitgliedskonten einsehen.

Wenn Sie registriert sind AWS Organizations, bestimmt Ihre Organisation ein Security Hub CSPM-Administratorkonto für die Organisation. Das Security Hub CSPM-Administratorkonto kann andere Organisationskonten als Mitgliedskonten aktivieren.

Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein. Ein Konto kann nur ein Administratorkonto haben.

Weitere Informationen finden Sie unter Verwaltung von Administrator- und Mitgliedskonten in Security Hub CSPM.

Administratorkonto

Ein Konto in Security Hub CSPM, dem Zugriff auf die Ergebnisse der zugehörigen Mitgliedskonten gewährt wird.

Ein Konto wird auf eine der folgenden Arten zu einem Administratorkonto:

- Das Konto lädt andere Konten ein, ihm in Security Hub CSPM zuzuordnen. Wenn diese Konten die Einladung annehmen, werden sie zu Mitgliedskonten und das einladende Konto wird zu ihrem Administratorkonto.
- Das Konto wird von einem Verwaltungskonto der Organisation als Security Hub CSPM-Administratorkonto festgelegt. Das Security Hub CSPM-Administratorkonto kann jedes Organisationskonto als Mitgliedskonto aktivieren und auch andere Konten als Mitgliedskonten einladen.

Ein Konto kann nur ein Administratorkonto haben. Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Region der Aggregation

Wenn Sie eine Aggregationsregion festlegen, können Sie die Sicherheitsergebnisse mehrerer Benutzer AWS-Regionen in einer einzigen Ansicht anzeigen.

Die Aggregationsregion ist die Region, von der aus Sie die Ergebnisse anzeigen und verwalten. Die Ergebnisse werden aus verknüpften Regionen zur Aggregationsregion zusammengefasst. Aktualisierungen der Ergebnisse werden regionsübergreifend repliziert.

In der Aggregationsregion enthalten die Seiten Sicherheitsstandards , Einblicke und Ergebnisse Daten aus allen verknüpften Regionen.

Weitere Informationen finden Sie unter the section called “Aggregation von Daten über Regionen hinweg”.

Archiviertes Ergebnis

Ein Ergebnis, dessen Datensatzstatus (`RecordState`) lautet`ARCHIVED`. Die Archivierung eines Ergebnisses bedeutet, dass der Findanbieter der Ansicht ist, dass das Ergebnis nicht mehr relevant ist. Der Datensatzstatus unterscheidet sich vom Workflow-Status, der den Status der Untersuchung eines Ergebnisses verfolgt.

Suchdienstleister können den BatchImportFindings Betrieb der Security Hub CSPM-API verwenden, um von ihnen erstellte Ergebnisse zu archivieren. Security Hub CSPM archiviert automatisch Kontrollergebnisse, die bestimmte Kriterien erfüllen. Weitere Informationen finden Sie unter Generierung, Aktualisierung und Archivierung von Kontrollbefunden.

Auf der Security Hub CSPM-Konsole schließen die Standardfiltereinstellungen archivierte Ergebnisse aus den Suchlisten und Tabellen aus. Sie können die Einstellungen aktualisieren, um archivierte Ergebnisse einzubeziehen. Wenn Sie Ergebnisse mithilfe der GetFindings Security Hub CSPM-API abrufen, ruft der Vorgang sowohl archivierte als auch aktive Ergebnisse ab. Um archivierte Ergebnisse auszuschließen, können Sie die Ergebnisse filtern. Beispiel:

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Format für Sicherheitsermittlungen (ASFF)

Ein standardisiertes Format für den Inhalt von Ergebnissen, die Security Hub CSPM aggregiert oder generiert. Mit dem AWS Security Finding Format können Sie Security Hub CSPM verwenden, um Ergebnisse anzuzeigen und zu analysieren, die von AWS Sicherheitsdiensten, Drittanbieterlösungen oder Security Hub CSPM selbst bei der Durchführung von Sicherheitsprüfungen generiert wurden. Weitere Informationen finden Sie unter AWS Format für Sicherheitssuche (ASFF).

Steuerung

Eine Schutz- oder Gegenmaßnahme, die für ein Informationssystem oder eine Organisation vorgeschrieben ist, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu

schützen und eine Reihe definierter Sicherheitsanforderungen zu erfüllen. Ein Sicherheitsstandard ist einer Sammlung von Kontrollen zugeordnet.

Der Begriff Sicherheitskontrolle bezieht sich auf Kontrollen, die in allen Standards eine einzige Kontroll-ID und einen einzigen Titel haben. Der Begriff Standardkontrolle bezieht sich auf Steuerelemente, die standardspezifische Kontroll-IDs und -Titel haben. Derzeit unterstützt Security Hub CSPM Standardkontrollen nur in den Regionen China und. AWS GovCloud (US) Regions Sicherheitskontrollen werden in allen anderen Regionen unterstützt.

Benutzerdefinierte Aktion

Ein Security Hub CSPM-Mechanismus zum Senden ausgewählter Ergebnisse an. EventBridge Eine benutzerdefinierte Aktion wird in Security Hub CSPM erstellt. Sie wird dann mit einer EventBridge Regel verknüpft. Die Regel definiert eine bestimmte Aktion, die ausgeführt werden soll, wenn Funde empfangen werden, die der benutzerdefinierten Aktions-ID zugeordnet sind. Benutzerdefinierte Aktionen können beispielsweise verwendet werden, um einen bestimmten Fund oder einen kleinen Satz von Funden an einen Antwort- oder Korrektur-Workflow zu senden. Weitere Informationen finden Sie unter the section called “Eine benutzerdefinierte Aktion erstellen”.

Delegiertes Administratorkonto (Organisationen)

In AWS Organizations ist das delegierte Administratorkonto für einen Dienst in der Lage, die Nutzung eines Dienstes für die Organisation zu verwalten.

In Security Hub CSPM ist das Security Hub CSPM-Administratorkonto auch das delegierte Administratorkonto für Security Hub CSPM. Wenn das Verwaltungskonto der Organisation zum ersten Mal ein Security Hub CSPM-Administratorkonto festlegt, ruft Security Hub CSPM die Organisationen an, um dieses Konto zum delegierten Administratorkonto zu machen.

Das Verwaltungskonto der Organisation muss dann das delegierte Administratorkonto als Security Hub CSPM-Administratorkonto in allen Regionen auswählen.

Erkenntnis

Der beobachtbare Datensatz einer Sicherheitsprüfung oder sicherheitsrelevanten Erkennung. Security Hub CSPM generiert und aktualisiert die Ergebnisse, nachdem die Sicherheitsüberprüfungen für Kontrollen abgeschlossen wurden. Diese werden als Kontrollergebnisse bezeichnet. Ergebnisse können auch aus Integrationen mit anderen Produkten AWS-Services und Produkten von Drittanbietern stammen.

Weitere Informationen finden Sie unter the section called “Ergebnisse”.

Cross-Region Aggregation

Die Zusammenfassung von Ergebnissen, Erkenntnissen, Kontrollkonformitätsstatus und Sicherheitsbewertungen aus verknüpften Regionen zu einer Aggregationsregion. Anschließend können Sie alle Ihre Daten aus der Aggregationsregion anzeigen und die Ergebnisse und Erkenntnisse aus der Aggregationsregion aktualisieren.

Weitere Informationen finden Sie unter the section called “Aggregation von Daten über Regionen hinweg”.

Auffinden der Aufnahme

Der Import von Ergebnissen aus anderen AWS Diensten und von Drittanbietern in Security Hub CSPM.

Das Auffinden von Ereignissen, bei denen eine Aufnahme aufgenommen wurde, umfasst sowohl neue Befunde als auch Aktualisierungen vorhandener Befunde.

Insight

Eine Sammlung zusammenhängender Funde, die durch eine Aggregationsanweisung und optionale Filter definiert wird. Ein Einblick identifiziert einen Sicherheitsbereich, der Aufmerksamkeit und Intervention erfordert. Security Hub CSPM bietet mehrere verwaltete (Standard-) Einblicke, die Sie nicht ändern können. Sie können auch benutzerdefinierte Security Hub CSPM-Einblicke erstellen, um Sicherheitsprobleme zu verfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind. Weitere Informationen finden Sie unter the section called “Insights”.

Verknüpfte Region

Wenn Sie die regionsübergreifende Aggregation aktivieren, ist eine verknüpfte Region eine Region, die Ergebnisse, Erkenntnisse, Kontrollkonformitätsstatus und Sicherheitsbewertungen in der Aggregationsregion zusammenfasst.

In einer verknüpften Region enthalten die Seiten „Ergebnisse“ und „Einblicke“ nur Ergebnisse aus dieser Region.

Weitere Informationen finden Sie unter the section called “Aggregation von Daten über Regionen hinweg”.

Mitgliedskonto

Ein Konto, das einem Administratorkonto die Erlaubnis erteilt hat, seine Ergebnisse einzusehen und entsprechende Maßnahmen zu ergreifen.

Ein Konto wird auf eine der folgenden Arten zu einem Mitgliedskonto:

- Das Konto akzeptiert eine Einladung von einem anderen Konto.
- Für ein Organisationskonto aktiviert das Security Hub CSPM-Administratorkonto das Konto als Mitgliedskonto.

Zugehörige Anforderungen

Eine Reihe von Branchen- oder regulatorischen Anforderungen, die einem Steuerelement zugeordnet sind.

Regel

Eine Reihe von automatisierten Kriterien, die verwendet werden, um zu beurteilen, ob ein Steuerelement eingehalten wird. Wenn eine Regel ausgewertet wird, kann sie erfolgreich sein oder fehlschlagen. Wenn die Auswertung nicht feststellen kann, ob die Regel erfolgreich ist oder fehlschlägt, befindet sich die Regel in einem Warnzustand. Wenn die Regel nicht ausgewertet werden kann, befindet sie sich in einem nicht verfügbaren Zustand.

Sicherheitsüberprüfung

Eine spezifische Bewertung einer Regel zu einem bestimmten Zeitpunkt anhand einer einzelnen Ressource, die zu einem Status`PASSED`,`FAILED`, `WARNING` oder führt. `NOT_AVAILABLE` Das Ausführen einer Sicherheitsprüfung führt zu einem Ergebnis.

Security Hub CSPM-Administratorkonto

Ein Organisationskonto, das die Security Hub CSPM-Mitgliedschaft für eine Organisation verwaltet.

Das Verwaltungskonto der Organisation bestimmt das Security Hub CSPM-Administratorkonto in jeder Region. Das Verwaltungskonto der Organisation muss in allen Regionen dasselbe Security Hub CSPM-Administratorkonto wählen.

Das Security Hub CSPM-Administratorkonto ist auch das delegierte Administratorkonto für Security Hub CSPM in Organisationen.

Das Security Hub CSPM-Administratorkonto kann jedes Organisationskonto als Mitgliedskonto aktivieren. Das Security Hub CSPM-Administratorkonto kann auch andere Konten als Mitgliedskonten einladen.

Sicherheitsstandard

Eine veröffentlichte Erklärung zu einem Thema, in der die Eigenschaften (in der Regel messbar und in Form von Kontrollen) definiert sind, die gegeben sein oder erreicht werden

müssen, um Compliance sicherzustellen. Sicherheitsstandards können auf regulatorischen Rahmenbedingungen, bewährten Methoden oder internen Unternehmensrichtlinien basieren. Ein Steuerelement kann einem oder mehreren unterstützten Standards in Security Hub CSPM zugeordnet sein. Weitere Informationen zu den Sicherheitsstandards in Security Hub CSPM finden Sie unter. Sicherheitsstandards in Security Hub CSPM verstehen

Schweregrad

Der einer Security Hub CSPM-Steuerung zugewiesene Schweregrad gibt an, wie wichtig die Kontrolle ist. Der Schweregrad einer Kontrolle kann „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ oder „Informativ“ sein. Der den Kontrollbefunden zugewiesene Schweregrad entspricht dem Schweregrad der Kontrolle selbst. Weitere Informationen darüber, wie Security Hub CSPM einer Kontrolle den Schweregrad zuweist, finden Sie unter. Schweregrade der Kontrollbefunde

Workflow-Status

Der Status einer Untersuchung zu einem Befund. Dies wird mithilfe des Attributs verfolgt. `Workflow.Status`

Der Workflow-Status ist zunächst `NEW`. Wenn Sie den Ressourcenbesitzer benachrichtigt haben, Maßnahmen für das Ergebnis zu ergreifen, können Sie den Workflow-Status auf `NOTIFIED` festlegen. Wenn die Suche kein Problem darstellt und keine Aktion erfordert, legen Sie den Workflow-Status auf `SUPPRESSED` fest. Nachdem Sie eine Suche überprüft und korrigiert haben, legen Sie den Workflow-Status auf `RESOLVED` fest.

Standardmäßig enthalten die meisten Suchlisten nur Ergebnisse mit dem Workflow-Status `NEW` oder `NOTIFIED`. Die Suche nach Listen für Steuerelemente umfasst auch `RESOLVED`-Ergebnisse.

Für die Operation GetFindings können Sie einen Filter für den Workflow-Status einschließen.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Die Security Hub CSPM-Konsole bietet eine Option zum Festlegen des Workflow-Status für Ergebnisse. Kunden (oder SIEM-, Ticketing-, Vorfallmanagement- oder SOAR-Tools, die im Auftrag eines Kunden Ergebnisse von Ergebnisanbietern aktualisieren) können mithilfe von BatchUpdateFindings auch den Workflow-Status aktualisieren.

Security Hub CSPM aktivieren

Es gibt zwei Möglichkeiten, AWS Security Hub CSPM zu aktivieren: durch Integration oder manuell. AWS Organizations

Wir empfehlen dringend die Integration mit Organisationen für Umgebungen mit mehreren Konten und mehreren Regionen. Wenn Sie ein eigenständiges Konto haben, müssen Sie Security Hub CSPM manuell einrichten.

Überprüfung der erforderlichen Berechtigungen

Nachdem Sie sich für Amazon Web Services (AWS) angemeldet haben, müssen Sie Security Hub CSPM aktivieren, um seine Funktionen und Funktionen nutzen zu können. Um Security Hub CSPM zu aktivieren, müssen Sie zunächst Berechtigungen einrichten, die Ihnen den Zugriff auf die Security Hub CSPM-Konsole und die API-Operationen ermöglichen. Sie oder Ihr AWS Administrator können dies tun, indem Sie AWS Identity and Access Management (IAM) verwenden, um die `AWSSecurityHubFullAccess` aufgerufene AWS verwaltete Richtlinie an Ihre IAM-Identität anzuhängen.

Um Security Hub CSPM über die Organisationsintegration zu aktivieren und zu verwalten, sollten Sie auch die verwaltete Richtlinie mit dem AWS Namen anhängen. `AWSSecurityHubOrganizationsAccess`

Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Security Hub.

Aktivierung von Security Hub CSPM mit der Organisationsintegration

Um Security Hub CSPM mit zu verwenden AWS Organizations, bestimmt das AWS Organizations Verwaltungskonto der Organisation ein Konto als delegiertes Security Hub CSPM-Administratorkonto für die Organisation. Security Hub CSPM wird automatisch im delegierten Administratorkonto in der aktuellen Region aktiviert.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Benennung des delegierten Administrators.

Security Hub CSPM console

So benennen Sie beim Onboarding den delegierten Security Hub CSPM-Administrator

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie Gehe zu Security Hub CSPM. Sie werden aufgefordert, sich beim Verwaltungskonto des Unternehmens anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator benennen im Abschnitt Delegiertes Administratorkonto das Konto des delegierten Administrators an. Wir empfehlen, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben.
4. Wählen Sie Als delegierten Administrator einrichten aus.

Security Hub CSPM API

Rufen Sie die `EnableOrganizationAdminAccount` API über das Verwaltungskonto der Organisation auf. Geben Sie die AWS-Konto ID des delegierten Administratorkontos für Security Hub CSPM an.

AWS CLI

Führen Sie den `enable-organization-admin-account` Befehl über das Verwaltungskonto der Organisation aus. Geben Sie die AWS-Konto ID des delegierten Administratorkontos für Security Hub CSPM ein.

Beispiel für einen Befehl:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Weitere Informationen zur Integration mit Organisationen finden Sie unterIntegration von Security Hub CSPM mitAWS Organizations.

Zentrale Konfiguration

Wenn Sie Security Hub CSPM und Organizations integrieren, haben Sie die Möglichkeit, eine Funktion namens zentrale Konfiguration zu verwenden, um Security Hub CSPM für Ihr Unternehmen einzurichten und zu verwalten. Wir empfehlen dringend, die zentrale Konfiguration zu

verwenden, da der Administrator so die Sicherheitsabdeckung für das Unternehmen anpassen kann. Gegebenenfalls kann der delegierte Administrator einem Mitgliedskonto gestatten, seine eigenen Sicherheitseinstellungen zu konfigurieren.

Die zentrale Konfiguration ermöglicht es dem delegierten Administrator, Security Hub CSPM für Konten, Organisationseinheiten und zu konfigurieren. AWS-Regionen Der delegierte Administrator konfiguriert Security Hub CSPM, indem er Konfigurationsrichtlinien erstellt. In einer Konfigurationsrichtlinie können Sie die folgenden Einstellungen angeben:

- Ob Security Hub CSPM aktiviert oder deaktiviert ist
- Welche Sicherheitsstandards sind aktiviert und deaktiviert
- Welche Sicherheitskontrollen sind aktiviert und deaktiviert
- Ob Parameter für ausgewählte Steuerelemente angepasst werden sollen

Als delegierter Administrator können Sie eine einzige Konfigurationsrichtlinie für Ihre gesamte Organisation oder verschiedene Konfigurationsrichtlinien für Ihre verschiedenen Konten und Organisationseinheiten erstellen. Beispielsweise können Testkonten und Produktionskonten unterschiedliche Konfigurationsrichtlinien verwenden.

Mitgliedskonten und Organisationseinheiten, die eine Konfigurationsrichtlinie verwenden, werden zentral verwaltet und können nur vom delegierten Administrator konfiguriert werden. Der delegierte Administrator kann bestimmte Mitgliedskonten und Organisationseinheiten als selbstverwaltet festlegen, sodass das Mitglied seine eigenen Einstellungen auf einer Grundlage konfigurieren kann. Region-by-Region

Wenn Sie keine zentrale Konfiguration verwenden, müssen Sie Security Hub CSPM in jedem Konto und jeder Region weitgehend separat konfigurieren. Dies wird als lokale Konfiguration bezeichnet. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und eine begrenzte Anzahl von Sicherheitsstandards in neuen Organisationskonten in der aktuellen Region automatisch aktivieren. Die lokale Konfiguration gilt nicht für bestehende Organisationskonten oder für andere Regionen als die aktuelle Region. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Manuelles Aktivieren von Security Hub CSPM

Sie müssen Security Hub CSPM manuell aktivieren, wenn Sie ein eigenständiges Konto haben oder wenn Sie es nicht integrieren. AWS Organizations Eigenständige Konten können nicht in Konten integriert werden AWS Organizations und müssen manuell aktiviert werden.

Wenn Sie Security Hub CSPM manuell aktivieren, legen Sie ein Security Hub CSPM-Administratorkonto fest und laden andere Konten ein, Mitgliedskonten zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub CSPM zu aktivieren. Wenn Sie Security Hub CSPM von der Konsole aus aktivieren, haben Sie auch die Möglichkeit, die unterstützten Sicherheitsstandards zu aktivieren.

Security Hub CSPM console

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wenn Sie die Security Hub CSPM-Konsole zum ersten Mal öffnen, wählen Sie Gehe zu Security Hub CSPM.
3. Auf der Willkommensseite sind im Abschnitt Sicherheitsstandards die Sicherheitsstandards aufgeführt, die Security Hub CSPM unterstützt.

   Markieren Sie das Kontrollkästchen für einen Standard, um ihn zu aktivieren, und deaktivieren Sie das Kontrollkästchen, um ihn zu deaktivieren.

   Sie können einen Standard oder seine einzelnen Steuerelemente jederzeit aktivieren oder deaktivieren. Informationen zur Verwaltung von Sicherheitsstandards finden Sie unterSicherheitsstandards in Security Hub CSPM verstehen.
4. Wählen Sie Enable Security Hub (Security Hub aktivieren).

Security Hub CSPM API

Rufen Sie die `EnableSecurityHub` API auf. Wenn Sie Security Hub CSPM über die API aktivieren, werden automatisch die folgenden Standardsicherheitsstandards aktiviert:

- AWS Grundlegende bewährte Methoden zur Sicherheit
- Benchmark v1.2.0 der AWS Foundations des Zentrums für Internetsicherheit (CIS)

Wenn Sie diese Standards nicht aktivieren möchten, setzen Sie `EnableDefaultStandards` auf `false`.

Sie können den `Tags` Parameter auch verwenden, um der Hub-Ressource Tag-Werte zuzuweisen.

AWS CLI

Führen Sie den Befehl `enable-security-hub` aus. Um die Standardstandards zu aktivieren, schließen Sie Folgendes ein`--enable-default-standards`. Um die Standardstandards nicht zu aktivieren, schließen Sie Folgendes ein`--no-enable-default-standards`. Die Standardsicherheitsstandards lauten wie folgt:

- AWS Grundlegende bewährte Sicherheitsmethoden
- Benchmark v1.2.0 der AWS Foundations des Zentrums für Internetsicherheit (CIS)

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Beispiel

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Multi-account Aktivierungsskript

> **Note**
>
> Anstelle dieses Skripts empfehlen wir, die zentrale Konfiguration zu verwenden, um Security Hub CSPM für mehrere Konten und Regionen zu aktivieren und zu konfigurieren.

Das Security Hub CSPM-Skript zur Aktivierung mehrerer Konten in GitHub ermöglicht es Ihnen, Security Hub CSPM konto- und regionsübergreifend zu aktivieren. Das Skript automatisiert auch das Senden und Aktivieren von Einladungen an Mitgliedskonten. AWS Config

Das Skript aktiviert automatisch die AWS Config Ressourcenaufzeichnung für alle Ressourcen, einschließlich globaler Ressourcen, in allen Regionen. Es beschränkt die Aufzeichnung globaler Ressourcen nicht auf eine einzelne Region. Um Kosten zu sparen, empfehlen wir, globale Ressourcen nur in einer einzigen Region zu erfassen. Wenn Sie die zentrale Konfiguration oder

die regionsübergreifende Aggregation verwenden, sollte dies Ihre Heimatregion sein. Weitere Informationen finden Sie unter Ressourcen aufzeichnen in AWS Config.

Es gibt ein entsprechendes Skript, um Security Hub CSPM konto- und regionsübergreifend zu deaktivieren.

Nächste Schritte: Bestandsmanagement und Integrationen

Nach der Aktivierung von Security Hub CSPM empfehlen wir, Sicherheitsstandards und -kontrollen zu aktivieren, um Ihren Sicherheitsstatus zu überwachen. Nachdem Sie die Kontrollen aktiviert haben, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsprüfungen und generiert Kontrollergebnisse, anhand derer Sie Fehlkonfigurationen in Ihrer Umgebung erkennen können. AWS Um Kontrollergebnisse zu erhalten, müssen Sie Security Hub CSPM aktivieren und konfigurieren AWS Config . Weitere Informationen finden Sie unter Aktivierung und Konfiguration AWS Config für Security Hub CSPM.

Nachdem Sie Security Hub CSPM aktiviert haben, können Sie auch Integrationen zwischen Security Hub CSPM und anderen AWS-Services Lösungen und Lösungen von Drittanbietern nutzen, um deren Ergebnisse in Security Hub CSPM einzusehen. Security Hub CSPM fasst Ergebnisse aus verschiedenen Quellen zusammen und nimmt sie in einem konsistenten Format auf. Weitere Informationen finden Sie unter Integrationen in Security Hub CSPM verstehen.

Aktivierung und Konfiguration AWS Config für Security Hub CSPM

AWS Security Hub CSPM verwendet AWS Config Regeln, um Sicherheitsprüfungen durchzuführen und Ergebnisse für die meisten Kontrollen zu generieren. AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem. AWS-Konto Es verwendet Regeln, um eine Basiskonfiguration für Ihre Ressourcen festzulegen, und einen Konfigurationsrekorder, um festzustellen, ob eine bestimmte Ressource gegen die Bedingungen einer Regel verstößt.

Einige Regeln, die als AWS Config verwaltete Regeln bezeichnet werden, sind vordefiniert und wurden von AWS Config entwickelt. Andere Regeln sind benutzerdefinierte AWS Config Regeln, die Security Hub CSPM entwickelt. AWS Config Regeln, die Security Hub CSPM für Kontrollen verwendet, werden als dienstbezogene Regeln bezeichnet. Service-linked Regeln ermöglichen es AWS-Services beispielsweise Security Hub CSPM, AWS Config Regeln in Ihrem Konto zu erstellen.

Wenn Sie sowohl AWS Security Hub CSPM als auch Security Hub aktiviert haben, erstellt Security Hub CSPM automatisch einen serviceverknüpften Konfigurationsrekorder, um Ihre Sicherheitskontrollen zu bewerten. Sie müssen ihn nicht manuell aktivieren oder konfigurieren.

AWS Config Weitere Informationen finden Sie unter Verwenden des serviceverknüpften Konfigurationsrekorders.

Wenn Sie Security Hub CSPM ohne Security Hub aktiviert haben, müssen Sie die Ressourcenaufzeichnung manuell aktivieren AWS Config und einschalten. Weitere Informationen finden Sie unter Manuelles Konfigurieren AWS Config.

Die auf dieser Seite beschriebenen AWS Config Voraussetzungen gelten nur für AWS Sicherheitsstandards wie AWS Foundational Security Best Practices und CIS AWS Foundations Benchmark. Multicloud-Standards wie CIS Azure Foundations Benchmark v4.0.0 erfordern nicht, dass Sie die AWS Config Aufzeichnung aktivieren oder einen Konfigurationsrekorder konfigurieren. Der Security Hub CSPM Multicloud-Connector richtet automatisch einen serviceverknüpften Rekorder zur Auswertung externer Cloud-Ressourcen ein. Die einzige Voraussetzung für Multicloud-Standards ist ein Security Hub CSPM-Connector für den externen Cloud-Anbieter.

Themen

- Verwenden des serviceverknüpften Konfigurationsrekorders
- Manuelles Konfigurieren AWS Config
- Die Steuerung verstehen Config.1
- Generierung von Regeln im Zusammenhang mit Diensten

Verwenden des serviceverknüpften Konfigurationsrekorders

Wenn Sie sowohl AWS Security Hub CSPM als auch Security Hub aktiviert haben, erstellt und verwaltet Security Hub CSPM automatisch einen serviceverknüpften Konfigurationsrekorder für Ihre Konten und Regionen. Sie müssen ihn nicht manuell aktivieren oder konfigurieren. AWS Config

Der Name dieses Konfigurationsrekorders lautet`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM erstellt für jedes Konto und jede Region, in der sowohl Security Hub CSPM als auch Security Hub aktiviert sind, einen entsprechenden serviceverknüpften Konfigurationsrekorder. Wenn Sie Security Hub CSPM für neue AWS-Konto s und AWS-Region s aktivieren, erstellt Security Hub CSPM automatisch den serviceverknüpften Konfigurationsrekorder.

Security Hub CSPM verwaltet die Ressourcenkonfiguration des serviceverknüpften Konfigurationsrekorders und stellt so sicher, dass die Aufzeichnung für alle Ressourcen aktiviert ist, die an die von Security Hub unterstützten Kontrollen gebunden sind. Eine Liste der erforderlichen Ressourcen finden Sie unter. Erforderlich AWS Config Ressourcen für Kontrollbefunde

Wenn Security Hub CSPM diesen serviceverknüpften Konfigurationsrekorder erstellt, verwendet Security Hub den vom Kunden verwalteten Konfigurationsrekorder nicht in. AWS Config

Weitere Informationen zu Konfigurationsrekordern finden Sie unter Arbeiten mit dem Konfigurationsrekorder im Entwicklerhandbuch.AWS Config

Manuelles Konfigurieren AWS Config

Die folgenden Schritte gelten, wenn Sie Security Hub CSPM ohne Security Hub aktiviert haben. In diesem Fall müssen Sie die Ressourcenaufzeichnung AWS Config für die Ressourcentypen, die von Ihren aktivierten Steuerelementen ausgewertet werden, für Ihr Konto aktivieren und die Ressourcenaufzeichnung einschalten. Danach erstellt Security Hub CSPM die entsprechenden AWS Config Regeln und beginnt mit der Durchführung von Sicherheitsprüfungen, um Ergebnisse zu generieren.

Überlegungen vor der Aktivierung und Konfiguration AWS Config

Um Kontrollergebnisse in Security Hub CSPM zu erhalten, AWS Config muss es für Ihr Konto in allen Ländern aktiviert sein, in AWS-Region denen Security Hub CSPM aktiviert ist. Wenn Sie Security Hub CSPM für eine Umgebung mit mehreren Konten verwenden, AWS Config muss es in jeder Region für das Administratorkonto und alle Mitgliedskonten aktiviert sein.

Wir empfehlen dringend, die Ressourcenaufzeichnung zu aktivieren, AWS Config bevor Sie die Security Hub CSPM-Standards und -Steuerelemente aktivieren. Auf diese Weise können Sie sicherstellen, dass Ihre Kontrollergebnisse korrekt sind.

Um die Ressourcenaufzeichnung in zu aktivieren AWS Config, müssen Sie über ausreichende Berechtigungen zum Aufzeichnen von Ressourcen in der AWS Identity and Access Management (IAM) -Rolle verfügen, die dem Konfigurationsrekorder zugeordnet ist. Stellen Sie außerdem sicher, dass keine IAM-Richtlinien oder AWS Organizations -Richtlinien AWS Config verhindern, dass Sie berechtigt sind, Ihre Ressourcen aufzuzeichnen. Security Hub CSPM-Steuerungen werten Ressourcenkonfigurationen direkt aus und berücksichtigen keine AWS Organizations Richtlinien. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter Arbeiten mit dem Konfigurationsrekorder im AWS Config Entwicklerhandbuch.

Wenn Sie einen Standard in Security Hub CSPM aktivieren, ihn aber nicht aktiviert haben AWS Config, versucht Security Hub CSPM, serviceverknüpfte AWS Config Regeln gemäß dem folgenden Zeitplan zu erstellen:

- An dem Tag, an dem Sie den Standard aktivieren.

- Am Tag, nachdem Sie den Standard aktiviert haben.
- 3 Tage nach der Aktivierung des Standards.
- 7 Tage nach der Aktivierung des Standards und danach kontinuierlich alle 7 Tage.

Wenn Sie die zentrale Konfiguration verwenden, versucht Security Hub CSPM jedes Mal, servicebezogene AWS Config Regeln zu erstellen, wenn Sie Konten, Organisationseinheiten (OUs) oder dem Stamm eine Konfigurationsrichtlinie zuordnen, die einen oder mehrere Standards aktiviert.

Ressourcen aufzeichnen in AWS Config

Bei der Aktivierung müssen Sie angeben AWS Config, welche AWS Ressourcen der AWS Config Konfigurationsrekorder aufzeichnen soll. Durch die serviceverknüpften Regeln ermöglicht der Konfigurationsrekorder Security Hub CSPM, Änderungen an Ihren Ressourcenkonfigurationen zu erkennen.

Damit Security Hub CSPM genaue Kontrollergebnisse generiert, müssen Sie die Aufzeichnung AWS Config für die Ressourcentypen aktivieren, die Ihren aktivierten Kontrollen entsprechen. Es handelt sich in erster Linie um aktivierte Steuerelemente mit einem durch Änderung ausgelösten Zeitplantyp, für den Ressourcen aufgezeichnet werden müssen. Für einige Steuerelemente mit einem periodischen Zeitplan ist auch die Erfassung von Ressourcen erforderlich. Eine Liste dieser Steuerelemente und der entsprechenden Ressourcen finden Sie unterErforderlich AWS Config Ressourcen für Kontrollbefunde.

Warning

Wenn Sie die AWS Config Aufzeichnung für Security Hub CSPM-Steuerelemente nicht korrekt konfigurieren, kann dies zu ungenauen Kontrollergebnissen führen, insbesondere in den folgenden Fällen:

- Sie haben die Ressource für ein bestimmtes Steuerelement nie aufgezeichnet, oder Sie haben die Aufzeichnung einer Ressource deaktiviert, bevor Sie diesen Ressourcentyp erstellt haben. In diesen Fällen erhalten Sie einen `WARNING` Befund für das fragliche Steuerelement, obwohl Sie möglicherweise Ressourcen im Bereich des Steuerelements erstellt haben, nachdem Sie die Aufzeichnung deaktiviert haben. Bei diesem `WARNING` Ergebnis handelt es sich um ein Standardergebnis, bei dem der Konfigurationsstatus der Ressource nicht wirklich bewertet wird.
- Sie deaktivieren die Aufzeichnung für eine Ressource, die von einem bestimmten Steuerelement ausgewertet wird. In diesem Fall behält Security Hub CSPM die

Kontrollergebnisse bei, die generiert wurden, bevor Sie die Aufzeichnung deaktiviert haben, obwohl das Steuerelement keine neuen oder aktualisierten Ressourcen auswertet. Security Hub CSPM ändert auch den Compliance-Status der Ergebnisse auf. `WARNING` Diese gespeicherten Ergebnisse geben möglicherweise nicht genau den aktuellen Konfigurationsstatus einer Ressource wieder.

AWS Config Zeichnet standardmäßig alle unterstützten regionalen Ressourcen auf, die es in der Umgebung entdeckt, AWS-Region in der es ausgeführt wird. Um alle Ergebnisse der Security Hub CSPM-Kontrolle zu erhalten, müssen Sie auch die Aufzeichnung globaler AWS Config Ressourcen konfigurieren. Um Kosten zu sparen, empfehlen wir, globale Ressourcen nur in einer einzigen Region zu erfassen. Wenn Sie die zentrale Konfiguration oder die regionsübergreifende Aggregation verwenden, sollte diese Region Ihre Heimatregion sein.

In AWS Config können Sie zwischen kontinuierlicher Aufzeichnung und täglicher Aufzeichnung von Änderungen des Ressourcenstatus wählen. Wenn Sie sich für die tägliche Aufzeichnung AWS Config entscheiden, werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann die Generierung von Security Hub CSPM-Ergebnissen für durch Änderungen ausgelöste Kontrollen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist.

Weitere Informationen zur AWS Config Aufzeichnung finden Sie im Entwicklerhandbuch unter Ressourcen aufzeichnen AWS.AWS Config

Möglichkeiten zur Aktivierung und Konfiguration AWS Config

Sie können die Ressourcenaufzeichnung auf eine der folgenden Arten aktivieren AWS Config und aktivieren:

- AWS Config Konsole — Sie können AWS Config die Aktivierung für ein Konto über die AWS Config Konsole vornehmen. Anweisungen finden Sie im AWS Config Entwicklerhandbuch unter Einrichtung AWS Config mit der Konsole.
- AWS CLI oder SDKs — Sie können sie AWS Config für ein Konto aktivieren, indem Sie AWS Command Line Interface (AWS CLI) verwenden. Eine Anleitung dazu finden Sie unter Einrichtung AWS Config mit dem AWS CLI im AWS Config Entwicklerhandbuch. AWS Software Development Kits (SDKs) sind auch für viele Programmiersprachen verfügbar.
- CloudFormation Vorlage — Zur Aktivierung AWS Config für viele Konten empfehlen wir, die AWS CloudFormation Vorlage mit dem Namen Enable AWS Config zu verwenden. Informationen zum

Zugriff auf diese Vorlage finden Sie in den AWS CloudFormation StackSet Beispielvorlagen im AWS CloudFormation Benutzerhandbuch.

Standardmäßig schließt diese Vorlage Aufzeichnungen für globale IAM-Ressourcen aus. Stellen Sie sicher, dass Sie die Aufzeichnung für globale IAM-Ressourcen nur in einer Version aktivieren, um Aufzeichnungskosten AWS-Region zu sparen. Wenn Sie die regionsübergreifende Aggregation aktiviert haben, sollte dies Ihre Security Hub CSPM-Heimatregion sein. Andernfalls kann es sich um jede Region handeln, in der Security Hub CSPM verfügbar ist und die Aufzeichnung globaler IAM-Ressourcen unterstützt. Wir empfehlen, eine StackSet zu verwenden, um alle Ressourcen, einschließlich der globalen IAM-Ressourcen, in der Heimatregion oder einer anderen ausgewählten Region aufzuzeichnen. Führen Sie dann eine Sekunde aus, StackSet um alle Ressourcen außer den globalen IAM-Ressourcen in anderen Regionen aufzuzeichnen.

- GitHub script — Security Hub CSPM bietet ein GitHubSkript, das Security Hub CSPM aktiviert, und zwar AWS Config für mehrere Konten in verschiedenen Regionen. Dieses Skript ist nützlich, wenn Sie es nicht integriert haben oder wenn Sie einige Mitgliedskonten haben AWS Organizations, die nicht Teil einer Organisation sind.

Weitere Informationen finden Sie im folgenden Blogbeitrag im AWS Sicherheitsblog: Optimieren Sie AWS Config für AWS Security Hub CSPM, um Ihre Cloud-Sicherheitslage effektiv zu verwalten.

Kostenüberlegungen

Security Hub CSPM kann sich auf Ihre Kosten für den AWS Config Konfigurationsrekorder auswirken, indem das `AWS::Config::ResourceCompliance` Konfigurationselement aktualisiert wird. Updates können jedes Mal erfolgen, wenn ein Security Hub CSPM-Steuerelement, das einer AWS Config Regel zugeordnet ist, den Konformitätsstatus ändert, aktiviert oder deaktiviert wird oder Parameter-Updates enthält. Wenn Sie den AWS Config Konfigurationsrekorder nur für Security Hub CSPM verwenden und dieses Konfigurationselement nicht für andere Zwecke verwenden, empfehlen wir, die Aufzeichnung dafür in zu deaktivieren. AWS Config Dies kann Ihre AWS Config Kosten senken. Sie müssen keine Aufzeichnungen machen, `AWS::Config::ResourceCompliance` damit Sicherheitsüberprüfungen in Security Hub CSPM funktionieren.

Informationen zu den Kosten im Zusammenhang mit der Ressourcenaufzeichnung finden Sie unter AWS Security Hub CSPM — Preise und AWS Config Preise.

Die Steuerung verstehen Config.1

> **Note**
>
> Wenn AWS Security Hub CSPM und Security Hub beide aktiviert sind, hat die Config.1 Steuerung immer den Status. `PASSED` Security Hub CSPM hat über einen serviceverknüpften Konfigurationsrekorder direkten Zugriff auf Konfigurationselemente. Weitere Informationen finden Sie unter Verwenden des serviceverknüpften Konfigurationsrekorders.

In Security Hub CSPM generiert das Config.1Steuerelement `FAILED` Ergebnisse in Ihrem Konto, wenn AWS Config es deaktiviert ist. Es generiert auch `FAILED` Ergebnisse in Ihrem Konto, wenn es aktiviert AWS Config ist, aber die Ressourcenaufzeichnung nicht aktiviert ist.

Wenn aktiviert AWS Config ist und die Ressourcenaufzeichnung aktiviert ist, die Ressourcenaufzeichnung jedoch nicht für einen Ressourcentyp aktiviert ist, den ein aktiviertes Steuerelement überprüft, generiert Security Hub CSPM einen `FAILED` Befund für das Config.1 Steuerelement. Zusätzlich zu diesem `FAILED` Ergebnis generiert Security Hub CSPM `WARNING` Ergebnisse für das aktivierte Steuerelement und die Arten von Ressourcen, die das Steuerelement überprüft. Wenn Sie beispielsweise die KMS.5Steuerung aktivieren und die Ressourcenaufzeichnung für nicht aktiviert ist AWS KMS keys, generiert Security Hub CSPM einen `FAILED` Befund für das Config.1 Steuerelement. Security Hub CSPM generiert auch `WARNING` Ergebnisse für die KMS.5 Steuerung und Ihre KMS-Schlüssel.

Um ein `PASSED` Ergebnis für das Config.1 Steuerelement zu erhalten, aktivieren Sie die Ressourcenaufzeichnung für alle Ressourcentypen, die den aktivierten Steuerelementen entsprechen. Deaktivieren Sie außerdem Steuerelemente, die für Ihre Organisation nicht erforderlich sind. Auf diese Weise können Sie sicherstellen, dass Ihre Sicherheitskontrollen keine Konfigurationslücken aufweisen. Außerdem können Sie so sicherstellen, dass Sie genaue Informationen zu falsch konfigurierten Ressourcen erhalten.

Wenn Sie der delegierte Security Hub CSPM-Administrator für eine Organisation sind, muss die AWS Config Aufzeichnung für Ihr Konto und Ihre Mitgliedskonten korrekt konfiguriert sein. Wenn Sie die regionsübergreifende Aggregation verwenden, muss die AWS Config Aufzeichnung in der Heimatregion und allen verknüpften Regionen korrekt konfiguriert sein. Globale Ressourcen müssen nicht in verknüpften Regionen aufgezeichnet werden.

Generierung von Regeln im Zusammenhang mit Diensten

Für jedes Steuerelement, das eine serviceverknüpfte AWS Config Regel verwendet, erstellt Security Hub CSPM Instanzen der erforderlichen Regel in Ihrer Umgebung. AWS

Diese serviceverknüpften Regeln sind spezifisch für Security Hub CSPM. Security Hub CSPM erstellt diese serviceverknüpften Regeln auch dann, wenn bereits andere Instanzen derselben Regeln existieren. Bei der serviceverknüpften Regel wird `securityhub` vor dem ursprünglichen Regelnamen und nach dem Regelnamen ein eindeutiger Bezeichner hinzugefügt. Für die AWS Config verwaltete Regel `vpc-flow-logs-enabled` könnte der Name der serviceverknüpften Regel beispielsweise lauten. `securityhub-vpc-flow-logs-enabled-12345`

Es gibt Kontingente für die Anzahl der AWS Config verwalteten Regeln, die zur Bewertung von Kontrollen verwendet werden können. AWS Config Regeln, die Security Hub CSPM erstellt, werden nicht auf diese Kontingente angerechnet. Sie können einen Sicherheitsstandard aktivieren, auch wenn Sie das AWS Config Kontingent für verwaltete Regeln in Ihrem Konto bereits erreicht haben. Weitere Informationen zu Kontingenten für AWS Config Regeln finden Sie unter Dienstbeschränkungen für AWS Config im AWS Config Entwicklerhandbuch.

> **Note**
>
> Wenn Sie Security Hub CSPM und Security Hub verwenden, können Sie die serviceverknüpften Regeln in sehen, AWS Config aber Sie können nicht sehen, welche kompatiblen oder nicht konformen Ressourcen mit der Regel verknüpft sind. Konforme und nicht konforme Ressourcen sind nur in Security Hub CSPM und Security Hub sichtbar.

Grundlegendes zur lokalen Konfiguration in Security Hub CSPM

Die lokale Konfiguration ist die Standardmethode, mit der eine AWS Organisation in Security Hub CSPM konfiguriert wird. Wenn Sie sich nicht für die zentrale Konfiguration entscheiden und diese aktivieren, verwendet Ihre Organisation standardmäßig die lokale Konfiguration.

Bei der lokalen Konfiguration hat das delegierte Security Hub CSPM-Administratorkonto eingeschränkte Kontrolle über die Konfigurationseinstellungen. Die einzigen Einstellungen, die der delegierte Administrator durchsetzen kann, sind die automatische Aktivierung von Security Hub CSPM und Standardsicherheitsstandards in neuen Unternehmenskonten. Diese Einstellungen gelten nur in der Region, in der Sie das delegierte Administratorkonto angegeben haben. Die Standardsicherheitsstandards sind AWS Foundational Security Best Practices (FSBP) und Center

for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Lokale Konfigurationseinstellungen gelten nicht für bestehende Organisationskonten oder für andere Regionen als die, für die das delegierte Administratorkonto eingerichtet wurde.

Neben der Aktivierung von Security Hub CSPM und Standardstandards in neuen Organisationskonten in einer einzelnen Region müssen Sie andere Security Hub CSPM-Einstellungen, einschließlich Standards und Kontrollen, für jede Region und jedes Konto separat konfigurieren. Da dies ein doppelter Vorgang sein kann, empfehlen wir, die zentrale Konfiguration für eine Umgebung mit mehreren Konten zu verwenden, wenn eine oder mehrere der folgenden Bedingungen auf Sie zutreffen:

- Sie möchten unterschiedliche Konfigurationseinstellungen für verschiedene Teile Ihrer Organisation (z. B. unterschiedliche aktivierte Standards oder Kontrollen für verschiedene Teams).
- Sie sind in mehreren Regionen tätig und möchten den Zeitaufwand und die Komplexität der Konfiguration des Dienstes in diesen Regionen reduzieren.
- Sie möchten, dass neue Konten bestimmte Konfigurationseinstellungen verwenden, wenn sie der Organisation beitreten.
- Sie möchten, dass Unternehmenskonten bestimmte Konfigurationseinstellungen von einem übergeordneten Konto oder einem Stammkonto erben.

Hinweise zur zentralen Konfiguration finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Grundlegendes zur zentralen Konfiguration in Security Hub CSPM

Die zentrale Konfiguration ist eine AWS Security Hub CSPM-Funktion, mit der Sie Security Hub CSPM für mehrere und einrichten und verwalten können. AWS-Konten AWS-Regionen Um die zentrale Konfiguration zu verwenden, müssen Sie zuerst Security Hub CSPM und integrieren. AWS Organizations Sie können die Dienste integrieren, indem Sie eine Organisation erstellen und ein delegiertes Security Hub CSPM-Administratorkonto für die Organisation festlegen.

Über das delegierte Security Hub CSPM-Administratorkonto können Sie Security Hub CSPM für die Konten und Organisationseinheiten (OUs) Ihrer Organisation in allen Regionen aktivieren. Sie können auch individuelle Sicherheitsstandards und Sicherheitskontrollen für Konten und Organisationseinheiten in allen Regionen aktivieren, konfigurieren und deaktivieren. Sie können diese Einstellungen in nur wenigen Schritten von einer Hauptregion aus konfigurieren, die als Heimatregion bezeichnet wird.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator auswählen, welche Konten und Organisationseinheiten konfiguriert werden sollen. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als selbstverwaltetes Konto festlegt, kann das Mitglied seine eigenen Einstellungen in jeder Region separat konfigurieren. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als zentral verwaltet festlegt, kann nur der delegierte Administrator das Mitgliedskonto oder die Organisationseinheit regionsübergreifend konfigurieren. Sie können alle Konten und Organisationseinheiten in Ihrer Organisation als zentral verwaltet, alle selbstverwaltet oder als eine Kombination aus beidem festlegen.

Um zentral verwaltete Konten zu konfigurieren, verwendet der delegierte Administrator die Security Hub CSPM-Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann der delegierte Administrator angeben, ob Security Hub CSPM aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert oder deaktiviert sind. Sie können auch verwendet werden, um Parameter für bestimmte Steuerelemente anzupassen.

Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Der delegierte Administrator gibt die Heimatregion der Organisation und die verknüpften Regionen an, bevor er die zentrale Konfiguration verwendet. Die Angabe verknüpfter Regionen ist optional. Der delegierte Administrator kann eine einzige Konfigurationsrichtlinie für die gesamte Organisation oder mehrere Konfigurationsrichtlinien erstellen, um variable Einstellungen für verschiedene Konten und Organisationseinheiten zu konfigurieren.

> **Tip**
>
> Wenn Sie keine zentrale Konfiguration verwenden, müssen Sie Security Hub CSPM für jedes Konto und jede Region weitgehend separat konfigurieren. Dies wird als lokale Konfiguration bezeichnet. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und eine begrenzte Anzahl von Sicherheitsstandards automatisch in neuen Unternehmenskonten in der aktuellen Region aktivieren. Die lokale Konfiguration gilt nicht für bestehende Organisationskonten oder für andere Regionen als die aktuelle Region. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Dieser Abschnitt bietet einen Überblick über die zentrale Konfiguration.

Vorteile der Verwendung der zentralen Konfiguration

Die zentrale Konfiguration bietet unter anderem folgende Vorteile:

Vereinfachen Sie die Konfiguration des Security Hub CSPM-Dienstes und der Funktionen

Wenn Sie die zentrale Konfiguration verwenden, führt Sie Security Hub CSPM durch den Prozess der Konfiguration bewährter Sicherheitsmethoden für Ihr Unternehmen. Außerdem werden die daraus resultierenden Konfigurationsrichtlinien automatisch für bestimmte Konten und Organisationseinheiten bereitgestellt. Wenn Sie über bestehende Security Hub CSPM-Einstellungen verfügen, z. B. die automatische Aktivierung neuer Sicherheitskontrollen, können Sie diese als Ausgangspunkt für Ihre Konfigurationsrichtlinien verwenden. Darüber hinaus wird auf der Konfigurationsseite der Security Hub CSPM-Konsole in Echtzeit eine Zusammenfassung Ihrer Konfigurationsrichtlinien angezeigt. Außerdem wird angezeigt, welche Konten und Organisationseinheiten die einzelnen Richtlinien verwenden.

Sie können die Konfiguration konto- und regionsübergreifend konfigurieren

Sie können die zentrale Konfiguration verwenden, um Security Hub CSPM für mehrere Konten und Regionen zu konfigurieren. Auf diese Weise können Sie sicherstellen, dass jeder Teil Ihres Unternehmens eine konsistente Konfiguration und einen angemessenen Sicherheitsschutz beibehält.

Passen Sie unterschiedliche Konfigurationen in unterschiedlichen Konten und Organisationseinheiten an

Bei der zentralen Konfiguration können Sie wählen, ob Sie die Konten und Organisationseinheiten Ihres Unternehmens auf unterschiedliche Weise konfigurieren möchten. Beispielsweise können für Ihre Testkonten und Produktionskonten unterschiedliche Konfigurationen erforderlich sein. Sie können auch eine Konfigurationsrichtlinie erstellen, die neue Konten abdeckt, wenn diese der Organisation beitreten.

Vermeiden Sie Konfigurationsabweichungen

Konfigurationsabweichungen treten auf, wenn ein Benutzer eine Änderung an einem Dienst oder einer Funktion vornimmt, die mit den Einstellungen des delegierten Administrators in Konflikt steht. Die zentrale Konfiguration verhindert diese Abweichung. Wenn Sie ein Konto oder eine Organisationseinheit als zentral verwaltet kennzeichnen, kann sie nur vom delegierten Administrator der Organisation konfiguriert werden. Wenn Sie es vorziehen, dass ein bestimmtes Konto oder eine bestimmte Organisationseinheit ihre eigenen Einstellungen konfiguriert, können Sie es als selbstverwaltet kennzeichnen.

Wann sollte die zentrale Konfiguration verwendet werden?

Die zentrale Konfiguration ist am vorteilhaftesten für AWS Umgebungen, die mehrere Security Hub CSPM-Konten enthalten. Es wurde entwickelt, um Ihnen zu helfen, Security Hub CSPM für mehrere Konten zentral zu verwalten.

Sie können die zentrale Konfiguration verwenden, um den Security Hub CSPM-Dienst, Sicherheitsstandards und Sicherheitskontrollen zu konfigurieren. Sie können es auch verwenden, um die Parameter bestimmter Steuerelemente anzupassen. Weitere Informationen zu Sicherheitsstandards finden Sie unterSicherheitsstandards in Security Hub CSPM verstehen. Weitere Informationen zu Sicherheitskontrollen finden Sie unterGrundlegendes zu den Sicherheitskontrollen in Security Hub CSPM.

Zentrale Begriffe und Konzepte zur Konfiguration

Wenn Sie die folgenden wichtigen Begriffe und Konzepte verstehen, können Sie die zentrale Konfiguration von Security Hub CSPM verwenden.

Zentrale Konfiguration

Eine Security Hub CSPM-Funktion, die dem delegierten Security Hub CSPM-Administratorkonto für eine Organisation hilft, den Security Hub CSPM-Dienst, Sicherheitsstandards und Sicherheitskontrollen für mehrere Konten und Regionen zu konfigurieren. Um diese Einstellungen zu konfigurieren, erstellt und verwaltet der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien für zentral verwaltete Konten in seiner Organisation. Self-managed Konten können ihre eigenen Einstellungen in jeder Region separat konfigurieren. Um die zentrale Konfiguration zu verwenden, müssen Sie Security Hub CSPM und integrieren. AWS Organizations

Heimatregion

AWS-Region Von dort aus konfiguriert der delegierte Administrator Security Hub CSPM zentral, indem er Konfigurationsrichtlinien erstellt und verwaltet. Konfigurationsrichtlinien gelten in der Heimatregion und allen verknüpften Regionen.

Die Heimatregion dient auch als Security Hub CSPM-Aggregationsregion und empfängt Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Eine Opt-in-Region kann nicht die Heimatregion sein, aber es kann

sich um eine verknüpfte Region handeln. Eine Liste der Regionen, für die Sie sich anmelden können, finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter Überlegungen vor dem Aktivieren und Deaktivieren von Regionen.

Verknüpfte Region

Und AWS-Region das kann von der Heimatregion aus konfiguriert werden. Konfigurationsrichtlinien werden vom delegierten Administrator in der Heimatregion erstellt. Die Richtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Die Angabe verknüpfter Regionen ist optional.

Eine verknüpfte Region sendet auch Ergebnisse, Erkenntnisse und andere Daten an die Heimatregion.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor eine Konfigurationsrichtlinie darauf angewendet werden kann. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Weitere Informationen finden Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Konten für AWS-Regionen Ihr AWS Konto verwendet werden können.

Ziel

Eine AWS-Konto, Organisationseinheit (OU) oder der Organisationsstamm.

Security Hub CSPM-Konfigurationsrichtlinie

Eine Sammlung von Security Hub CSPM-Einstellungen, die der delegierte Administrator für zentral verwaltete Ziele konfigurieren kann. Dies umfasst:

- Ob Security Hub CSPM aktiviert oder deaktiviert werden soll.
- Ob ein oder mehrere Sicherheitsstandards aktiviert werden sollen.
- Welche Sicherheitskontrollen für alle aktivierten Standards aktiviert werden sollen. Der delegierte Administrator kann dies tun, indem er eine Liste bestimmter Kontrollen bereitstellt, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Kontrollen (einschließlich neuer Kontrollen, wenn sie veröffentlicht werden). Alternativ kann der delegierte Administrator eine Liste bestimmter Kontrollen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen (einschließlich neuer Kontrollen, wenn sie veröffentlicht werden).
- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente in allen aktivierten Standards an.

Eine Konfigurationsrichtlinie wird in der Heimatregion und allen verknüpften Regionen wirksam, nachdem sie mindestens einem Konto, einer Organisationseinheit (OU) oder dem Stammverzeichnis zugeordnet wurde.

Auf der Security Hub CSPM-Konsole kann der delegierte Administrator die von Security Hub CSPM empfohlene Konfigurationsrichtlinie auswählen oder benutzerdefinierte Konfigurationsrichtlinien erstellen. Mit der Security Hub CSPM-API und AWS CLI kann der delegierte Administrator nur benutzerdefinierte Konfigurationsrichtlinien erstellen. Der delegierte Administrator kann maximal 20 benutzerdefinierte Konfigurationsrichtlinien erstellen.

In der empfohlenen Konfigurationsrichtlinie sind Security Hub CSPM, der Standard AWS Foundational Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente aktiviert. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Konfigurationsrichtlinie gilt für die gesamte Organisation.

Um unterschiedliche Einstellungen auf die Organisation anzuwenden oder unterschiedliche Konfigurationsrichtlinien auf verschiedene Konten und Organisationseinheiten anzuwenden, erstellen Sie eine benutzerdefinierte Konfigurationsrichtlinie.

> **Note**
>
> Konfigurationsrichtlinien unterstützen nur AWS Sicherheitsstandards und Kontrollen. Multicloud-Standards wie CIS Azure Foundations Benchmark v4.0.0 und die zugehörigen Multicloud-Steuerelemente können nicht in eine Konfigurationsrichtlinie aufgenommen werden. Um Multicloud-Standards zu aktivieren oder zu konfigurieren, verwenden Sie lokale Konfigurationsmechanismen direkt in der gewünschten Version. AWS-Konto

Lokale Konfiguration

Der Standardkonfigurationstyp für eine Organisation nach der Integration von Security Hub CSPM und. AWS Organizations Bei der lokalen Konfiguration kann der delegierte Administrator festlegen, dass Security Hub CSPM und Standardsicherheitsstandards in neuen Unternehmenskonten in der aktuellen Region automatisch aktiviert werden. Wenn der delegierte Administrator automatisch Standardstandards aktiviert, werden alle Kontrollen, die Teil dieser Standards sind, auch automatisch mit Standardparametern für neue Organisationskonten aktiviert. Diese Einstellungen gelten nicht für bestehende Konten, sodass es nach dem Beitritt eines Kontos zur Organisation zu Konfigurationsabweichungen kommen kann. Die Deaktivierung bestimmter

Kontrollen, die Teil der Standardstandards sind, und die Konfiguration zusätzlicher Standards und Kontrollen müssen für jedes Konto und jede Region separat erfolgen.

Die lokale Konfiguration unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Um Konfigurationsrichtlinien zu verwenden, müssen Sie zur zentralen Konfiguration wechseln.

Manuelle Kontoverwaltung

Wenn Sie Security Hub CSPM nicht in Security Hub integrieren AWS Organizations oder ein eigenständiges Konto haben, müssen Sie die Einstellungen für jedes Konto in jeder Region separat angeben. Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht.

Zentrale Konfigurations-APIs

Security Hub CSPM-Operationen, die nur der vom Security Hub CSPM delegierte Security Hub CSPM-Administrator in der Heimatregion verwenden kann, um Konfigurationsrichtlinien für zentral verwaltete Konten zu verwalten. Zu den Vorgängen gehören:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Account-specific APIs

Security Hub CSPM-Operationen, mit denen Security Hub CSPM, Standards und Kontrollen für jedes Konto aktiviert oder deaktiviert werden können. Diese Operationen werden in jeder einzelnen Region verwendet.

Self-managed Konten können kontospezifische Operationen verwenden, um ihre eigenen Einstellungen zu konfigurieren. Zentral verwaltete Konten können die folgenden kontospezifischen Operationen in der Heimatregion und verknüpften Regionen nicht verwenden. In diesen

Regionen kann nur der delegierte Administrator zentral verwaltete Konten über zentrale Konfigurationsvorgänge und Konfigurationsrichtlinien konfigurieren.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Um den Kontostatus zu überprüfen, kann der Besitzer eines zentral verwalteten Kontos `Get` beliebige `Describe` Operationen der Security Hub CSPM-API verwenden.

Wenn Sie statt der zentralen Konfiguration die lokale Konfiguration oder die manuelle Kontoverwaltung verwenden, können Sie diese kontospezifischen Operationen verwenden.

Self-managed Konten können auch AND-Operationen verwenden`*Invitations`. `*Members` Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden. Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Organisationseinheit (OU)

In AWS Organizations und Security Hub CSPM, ein Container für eine Gruppe von. AWS-Konten Eine Organisationseinheit (OU) kann auch andere OUs enthalten, sodass Sie eine Hierarchie erstellen können, die einem umgedrehten Baum ähnelt, mit einer übergeordneten Organisationseinheit an der Spitze und Zweigen von OUs, die nach unten reichen und in Konten enden, die Blätter des Baums sind. Eine Organisationseinheit kann genau eine übergeordnete Organisationseinheit haben, und jedes Organisationskonto kann Mitglied genau einer Organisationseinheit sein.

Sie können Organisationseinheiten in AWS Organizations oder verwalten AWS Control Tower. Weitere Informationen finden Sie unter Verwaltung von Organisationseinheiten im AWS Organizations Benutzerhandbuch oder Verwaltung von Organisationen und Konten mit AWS Control Tower im AWS Control Tower Benutzerhandbuch.

Der delegierte Administrator kann Konfigurationsrichtlinien bestimmten Konten oder Organisationseinheiten oder dem Stamm zuordnen, sodass alle Konten und Organisationseinheiten in einer Organisation abgedeckt werden.

Zentral verwaltet

Ein Ziel, das nur der delegierte Administrator mithilfe von Konfigurationsrichtlinien regionsübergreifend konfigurieren kann.

Das delegierte Administratorkonto gibt an, ob ein Ziel zentral verwaltet wird. Der delegierte Administrator kann auch den Status eines Ziels von zentral verwaltet in selbstverwaltet ändern oder umgekehrt.

Self-managed

Ein Ziel, das seine eigenen Security Hub CSPM-Einstellungen verwaltet. Ein selbstverwaltetes Ziel verwendet kontospezifische Operationen, um Security Hub CSPM für sich selbst in jeder Region separat zu konfigurieren. Dies steht im Gegensatz zu zentral verwalteten Zielen, die nur vom delegierten Administrator regionsübergreifend über Konfigurationsrichtlinien konfiguriert werden können.

Das delegierte Administratorkonto gibt an, ob ein Ziel selbst verwaltet wird. Der delegierte Administrator kann selbstverwaltetes Verhalten auf ein Ziel anwenden. Alternativ kann ein Konto oder eine Organisationseinheit das selbstverwaltete Verhalten von einem Elternteil erben.

Das delegierte Administratorkonto kann selbst ein selbstverwaltetes Konto sein. Das delegierte Administratorkonto kann den Status eines Ziels von selbstverwaltet in zentral verwaltet ändern oder umgekehrt.

Zuordnung von Konfigurationsrichtlinien

Eine Verknüpfung zwischen einer Konfigurationsrichtlinie und einem Konto, einer Organisationseinheit (OU) oder einem Stamm. Wenn eine Richtlinienzuordnung vorhanden ist, verwendet das Konto, die Organisationseinheit oder das Stammverzeichnis die in der Konfigurationsrichtlinie definierten Einstellungen. In einem der folgenden Fälle besteht eine Zuordnung:

- Wenn der delegierte Administrator eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder einen Root-Benutzer anwendet
- Wenn ein Konto oder eine Organisationseinheit eine Konfigurationsrichtlinie von einer übergeordneten Organisationseinheit oder der Stammorganisation erbt

Eine Zuordnung besteht, bis eine andere Konfiguration angewendet oder vererbt wird.

Angewendete Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der der delegierte Administrator eine Konfigurationsrichtlinie direkt auf Zielkonten, Organisationseinheiten oder das Stammkonto anwendet. Ziele werden so konfiguriert, wie sie in der Konfigurationsrichtlinie definiert sind, und nur der delegierte Administrator kann ihre Konfiguration ändern. Wenn die Konfigurationsrichtlinie auf das Stammverzeichnis angewendet wird, wirkt sie sich auf alle Konten und Organisationseinheiten in der Organisation aus, die keine andere Konfiguration aufgrund von Anwendungen oder Vererbung durch das nächstgelegene übergeordnete Unternehmen verwenden.

Der delegierte Administrator kann eine selbstverwaltete Konfiguration auch auf bestimmte Konten, Organisationseinheiten oder das Stammverzeichnis anwenden.

Geerbte Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der ein Konto oder eine Organisationseinheit die Konfiguration der nächstgelegenen übergeordneten Organisationseinheit oder der Stammorganisation übernimmt. Wenn eine Konfigurationsrichtlinie nicht direkt auf ein Konto oder eine Organisationseinheit angewendet wird, erbt sie die Konfiguration der nächstgelegenen übergeordneten Organisation. Alle Elemente einer Richtlinie werden vererbt. Mit anderen Worten, ein Konto oder eine Organisationseinheit kann sich nicht dafür entscheiden, selektiv nur Teile einer Richtlinie zu erben. Wenn der nächstgelegene Elternteil selbst verwaltet wird, erbt das untergeordnete Konto oder die Organisationseinheit das selbstverwaltete Verhalten des Elternteils.

Die Vererbung kann eine angewendete Konfiguration nicht außer Kraft setzen. Das heißt, wenn eine Konfigurationsrichtlinie oder eine selbstverwaltete Konfiguration direkt auf ein Konto oder eine Organisationseinheit angewendet wird, verwendet sie diese Konfiguration und erbt nicht die Konfiguration der übergeordneten Einheit.

Root

In AWS Organizations und Security Hub CSPM, dem übergeordneten Knoten der obersten Ebene in einer Organisation. Wenn der delegierte Administrator eine Konfigurationsrichtlinie auf Root anwendet, wird die Richtlinie allen Konten und Organisationseinheiten in der Organisation zugeordnet, es sei denn, sie verwenden aufgrund von Anwendung oder Vererbung eine andere Richtlinie oder sind als selbstverwaltet gekennzeichnet. Wenn der Administrator das Stammverzeichnis als selbstverwaltet festlegt, werden alle Konten und Organisationseinheiten in der Organisation selbst verwaltet, es sei denn, sie verwenden eine Konfigurationsrichtlinie durch

Anwendung oder Vererbung. Wenn das Stammverzeichnis selbst verwaltet wird und derzeit keine Konfigurationsrichtlinien existieren, behalten alle neuen Konten in der Organisation ihre aktuellen Einstellungen bei.

Neue Konten, die einer Organisation beitreten, fallen unter das Stammkonto, bis sie einer bestimmten Organisationseinheit zugewiesen werden. Wenn ein neues Konto keiner Organisationseinheit zugewiesen ist, erbt es die Stammkonfiguration, es sei denn, der delegierte Administrator bestimmt es als selbstverwaltetes Konto.

Aktivierung der zentralen Konfiguration in Security Hub CSPM

Das delegierte AWS Security Hub CSPM-Administratorkonto kann die zentrale Konfiguration verwenden, um Security Hub CSPM, Standards und Kontrollen für mehrere Konten und Organisationseinheiten (OUs) zu konfigurieren. AWS-Regionen

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter. Grundlegendes zur zentralen Konfiguration in Security Hub CSPM

In diesem Abschnitt werden die Voraussetzungen für die zentrale Konfiguration und die ersten Schritte zur Verwendung dieser Konfiguration erläutert.

Voraussetzungen für die zentrale Konfiguration

Bevor Sie die zentrale Konfiguration verwenden können, müssen Sie Security Hub CSPM in die Heimatregion integrieren AWS Organizations und eine Heimatregion festlegen. Wenn Sie die Security Hub CSPM-Konsole verwenden, sind diese Voraussetzungen im Opt-in-Workflow für die zentrale Konfiguration enthalten.

In Organizations integrieren

Sie müssen Security Hub CSPM und Organizations integrieren, um die zentrale Konfiguration verwenden zu können.

Um diese Dienste zu integrieren, erstellen Sie zunächst eine Organisation in Organizations. Über das Verwaltungskonto der Organizations bestimmen Sie dann ein delegiertes Security Hub-CSPM-Administratorkonto. Detaillierte Anweisungen finden Sie unter Integration von Security Hub CSPM mitAWS Organizations.

Stellen Sie sicher, dass Sie Ihren delegierten Administrator in Ihrer gewünschten Heimatregion angeben. Wenn Sie die zentrale Konfiguration verwenden, wird derselbe delegierte Administrator

automatisch auch in allen verknüpften Regionen eingerichtet. Das Organisationsverwaltungskonto kann nicht als delegiertes Administratorkonto festgelegt werden.

> **Important**
>
> Wenn Sie die zentrale Konfiguration verwenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-APIs nicht verwenden, um das delegierte Administratorkonto zu ändern oder zu entfernen. Wenn das Verwaltungskonto der Organizations AWS Organizations APIs verwendet, um den delegierten Security Hub CSPM-Administrator zu ändern oder zu entfernen, stoppt Security Hub CSPM automatisch die zentrale Konfiguration. Ihre Konfigurationsrichtlinien werden ebenfalls getrennt und gelöscht. Mitgliedskonten behalten die Konfiguration bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Geben Sie eine Heimatregion an

Sie müssen eine Heimatregion angeben, um die zentrale Konfiguration verwenden zu können. Die Heimatregion ist die Region, von der aus der delegierte Administrator die Organisation konfiguriert.

> **Note**
>
> Bei der Heimatregion kann es sich nicht um eine Region handeln, die als Opt-in-Region ausgewiesen AWS wurde. Eine Opt-in-Region ist standardmäßig deaktiviert. Eine Liste der Opt-in-Regionen finden Sie unter Überlegungen vor der Aktivierung und Deaktivierung von Regionen im Referenzhandbuch zur AWSKontoverwaltung.

Optional können Sie eine oder mehrere verknüpfte Regionen angeben, die von der Heimatregion aus konfiguriert werden können.

Der delegierte Administrator kann Konfigurationsrichtlinien nur von der Heimatregion aus erstellen und verwalten. Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur für eine Teilmenge dieser Regionen gilt und nicht für andere. Eine Ausnahme bilden Kontrollen, die globale Ressourcen betreffen. Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Weitere Informationen finden Sie unter Steuerungen, die globale Ressourcen verwenden.

Die Heimatregion ist auch Ihre Security Hub-CSPM-Aggregationsregion, die Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen erhält.

Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt haben, ist dies Ihre Standard-Heimatregion für die zentrale Konfiguration. Sie können die Heimatregion ändern, bevor Sie die zentrale Konfiguration verwenden, indem Sie Ihren aktuellen Suchaggregator löschen und einen neuen in der gewünschten Heimatregion erstellen. Ein Findingaggregator ist eine Security Hub-CSPM-Ressource, die die Heimatregion und verknüpfte Regionen spezifiziert.

Informationen zur Festlegung einer Heimatregion finden Sie in den Schritten zum Einstellen einer Aggregationsregion. Wenn Sie bereits eine Heimatregion haben, können Sie die GetFindingAggregatorAPI aufrufen, um Details zu dieser Region zu sehen, einschließlich der Regionen, die derzeit damit verknüpft sind.

Anweisungen zur Aktivierung der zentralen Konfiguration

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die zentrale Konfiguration für Ihr Unternehmen zu aktivieren.

Security Hub CSPM console

Um die zentrale Konfiguration (Konsole) zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus. Wählen Sie dann Zentrale Konfiguration starten aus.

   Wenn Sie bei Security Hub CSPM einsteigen, wählen Sie Gehe zu Security Hub CSPM.
3. Wählen Sie auf der Seite Delegierten Administrator benennen Ihr delegiertes Administratorkonto aus oder geben Sie dessen Konto-ID ein. Falls zutreffend, empfehlen wir, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben. Wählen Sie Als delegierten Administrator festlegen aus.
4. Wählen Sie auf der Seite Organisation zentralisieren im Abschnitt Regionen Ihre Heimatregion aus. Sie müssen in der Heimatregion angemeldet sein, um fortzufahren. Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt haben, wird diese als Heimatregion angezeigt. Um die Heimatregion zu ändern, wählen

Sie „Regionseinstellungen bearbeiten“. Sie können dann Ihre bevorzugte Heimatregion auswählen und zu diesem Workflow zurückkehren.

5. Wählen Sie mindestens eine Region aus, um eine Verknüpfung mit der Heimatregion herzustellen. Wählen Sie optional aus, ob Sie future unterstützte Regionen automatisch mit der Heimatregion verknüpfen möchten. Die Regionen, die Sie hier auswählen, werden vom delegierten Administrator von der Heimatregion aus konfiguriert. Die Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen.
6. Wählen Sie Bestätigen und fortfahren.
7. Sie können jetzt die zentrale Konfiguration verwenden. Folgen Sie weiterhin den Anweisungen der Konsole, um Ihre erste Konfigurationsrichtlinie zu erstellen. Wenn Sie noch nicht bereit sind, eine Konfigurationsrichtlinie zu erstellen, wählen Sie Ich bin noch nicht bereit zur Konfiguration. Sie können später eine Richtlinie erstellen, indem Sie im Navigationsbereich Einstellungen und Konfiguration auswählen. Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unterKonfigurationsrichtlinien erstellen und zuordnen.

Security Hub CSPM API

So aktivieren Sie die zentrale Konfiguration (API)

1. Rufen Sie die UpdateOrganizationConfigurationAPI mit den Anmeldeinformationen des delegierten Administratorkontos von der Heimatregion aus auf.
2. Stellen Sie das `AutoEnable` Feld auf ein. `false`
3. Stellen Sie das `ConfigurationType` Feld im `OrganizationConfiguration` Objekt auf ein`CENTRAL`. Diese Aktion hat folgende Auswirkungen:

   - Benennt das anrufende Konto als delegierten Security Hub-CSPM-Administrator in allen verknüpften Regionen.
   - Aktiviert Security Hub CSPM im delegierten Administratorkonto in allen verknüpften Regionen.
   - Benennt das anrufende Konto als delegierten Security Hub CSPM-Administrator für neue und bestehende Konten, die Security Hub CSPM verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub CSPM aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für

bestehende Organisationskonten eingerichtet, wenn Security Hub CSPM bereits aktiviert ist.

- Stellt AutoEnable`false`in allen verknüpften Regionen und AutoEnableStandardsauf `NONE` in der Heimatregion und allen verknüpften Regionen ein. Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub CSPM und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.

4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM in Ihrer Organisation zu konfigurieren. Anweisungen zur Erstellung einer Konfigurationsrichtlinie finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

Beispiel für eine API-Anfrage:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Um die zentrale Konfiguration zu aktivieren (AWS CLI)

1. Führen Sie den update-organization-configurationBefehl mit den Anmeldeinformationen des delegierten Administratorkontos in der Heimatregion aus.
2. Schließen Sie den Parameter `no-auto-enable` ein.
3. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf `CENTRAL` ein. Diese Aktion hat folgende Auswirkungen:

   - Benennt das anrufende Konto als delegierten Security Hub-CSPM-Administrator in allen verknüpften Regionen.
   - Aktiviert Security Hub CSPM im delegierten Administratorkonto in allen verknüpften Regionen.

- Benennt das anrufende Konto als delegierten Security Hub CSPM-Administrator für neue und bestehende Konten, die Security Hub CSPM verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für bestehende Organisationskonten eingerichtet, wenn Security Hub CSPM bereits aktiviert ist.
- Legt die Option zur automatischen Aktivierung no-auto-enablein allen verknüpften Regionen und auf `NONE` in der Heimatregion und allen verknüpften Regionen fest auto-enable-standards. Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub CSPM und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.

4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM in Ihrer Organisation zu konfigurieren. Anweisungen zur Erstellung einer Konfigurationsrichtlinie finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

Beispielbefehl:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Zentral verwaltete Ziele im Vergleich zu selbstverwalteten Zielen

Wenn Sie die zentrale Konfiguration aktivieren, kann der delegierte AWS Security Hub CSPM-Administrator jedes Organisationskonto, jede Organisationseinheit (OU) und den Stamm als zentral verwaltet oder selbstverwaltet festlegen. Der Verwaltungstyp eines Ziels bestimmt, wie Sie seine Security Hub CSPM-Einstellungen angeben können.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter. Grundlegendes zur zentralen Konfiguration in Security Hub CSPM

In diesem Abschnitt werden die Unterschiede zwischen einer zentral verwalteten und einer selbstverwalteten Bezeichnung sowie die Auswahl des Verwaltungstyps eines Kontos, einer Organisationseinheit oder eines Stammkontos erläutert.

Self-managed

Der Besitzer eines selbstverwalteten Kontos, einer Organisationseinheit oder eines Stammkontos muss die Einstellungen für jedes Konto separat konfigurieren. AWS-Region Der delegierte Administrator kann keine Konfigurationsrichtlinien für selbstverwaltete Ziele erstellen.

Zentral verwaltet

Nur der delegierte Security Hub CSPM-Administrator kann Einstellungen für zentral verwaltete Konten, Organisationseinheiten oder das Stammkonto in der Heimatregion und den verknüpften Regionen konfigurieren. Konfigurationsrichtlinien können zentral verwalteten Konten und Organisationseinheiten zugeordnet werden.

Der delegierte Administrator kann den Status eines Ziels zwischen selbstverwaltetem und zentral verwaltetem ändern. Standardmäßig werden alle Konten und Organisationseinheiten selbst verwaltet, wenn Sie die zentrale Konfiguration über die Security Hub CSPM-API starten. In der Konsole hängt der Verwaltungstyp von Ihrer ersten Konfigurationsrichtlinie ab. Konten und Organisationseinheiten, die Sie Ihrer ersten Richtlinie zuordnen, werden zentral verwaltet. Andere Konten und Organisationseinheiten werden standardmäßig selbst verwaltet.

Wenn Sie einem zuvor selbstverwalteten Konto eine Konfigurationsrichtlinie zuordnen, haben die Richtlinieneinstellungen Vorrang vor der Bezeichnung für selbstverwaltetes Konto. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Wenn Sie ein zentral verwaltetes Konto in ein selbstverwaltetes Konto ändern, bleiben die Einstellungen, die zuvor über eine Konfigurationsrichtlinie auf das Konto angewendet wurden, bestehen. Beispielsweise könnte ein zentral verwaltetes Konto zunächst mit einer Richtlinie verknüpft werden, die Security Hub CSPM aktiviert, AWS Foundational Security Best Practices aktiviert und deaktiviert. CloudTrail.1 Wenn Sie das Konto dann als selbstverwaltet kennzeichnen, bleiben alle Einstellungen unverändert. Der Kontoinhaber kann die Einstellungen für das Konto in Zukunft jedoch unabhängig ändern.

Kinderkonten und Organisationseinheiten können das selbstverwaltete Verhalten von einem selbstverwalteten Elternteil erben, genauso wie untergeordnete Konten und Organisationseinheiten Konfigurationsrichtlinien von zentral verwalteten übergeordneten Konten erben können. Weitere Informationen finden Sie unter Richtlinienverknüpfung durch Anwendung und Vererbung.

Ein selbstverwaltetes Konto oder eine Organisationseinheit kann keine Konfigurationsrichtlinie von einem übergeordneten Knoten oder vom Stammknoten erben. Wenn Sie beispielsweise möchten, dass alle Konten und Organisationseinheiten in Ihrer Organisation eine Konfigurationsrichtlinie vom Stammverzeichnis erben, müssen Sie den Verwaltungstyp für selbstverwaltete Knoten auf zentral verwaltete Knoten ändern.

Optionen zum Konfigurieren von Einstellungen in selbstverwalteten Konten

Self-managed Konten müssen ihre eigenen Einstellungen in jeder Region separat konfigurieren.

Besitzer von selbstverwalteten Konten können die folgenden Operationen der Security Hub CSPM-API in jeder Region aufrufen, um ihre Einstellungen zu konfigurieren:

- `EnableSecurityHub`und `DisableSecurityHub` um den Security Hub CSPM-Dienst zu aktivieren oder zu deaktivieren (wenn ein selbstverwaltetes Konto über einen delegierten Security Hub CSPM-Administrator verfügt, muss der Administrator die Kontozuweisung aufheben, bevor der Kontoinhaber Security Hub CSPM deaktivieren kann).
- `BatchEnableStandards`und `BatchDisableStandards` um Standards zu aktivieren oder zu deaktivieren
- `BatchUpdateStandardsControlAssociations`oder `UpdateStandardsControl` um Steuerungen zu aktivieren oder zu deaktivieren

Self-managed Konten können auch `*Invitations` `*Members` AND-Operationen verwenden. Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden. Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Eine Beschreibung der Security Hub CSPM API-Aktionen finden Sie in der AWSSecurity Hub CSPM API-Referenz.

Self-managed Konten können auch die Security Hub CSPM-Konsole verwenden oder AWS CLI ihre Einstellungen in jeder Region konfigurieren.

Self-managed Konten können keine APIs aufrufen, die sich auf Security Hub CSPM-Konfigurationsrichtlinien und Richtlinienzuordnungen beziehen. Nur der delegierte Administrator kann zentrale Konfigurations-APIs aufrufen und Konfigurationsrichtlinien verwenden, um zentral verwaltete Konten zu konfigurieren.

Auswahl des Verwaltungstyps eines Ziels

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto oder eine Organisationseinheit in AWS Security Hub CSPM als zentral verwaltet oder selbstverwaltet zu kennzeichnen.

Security Hub CSPM console

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie Konfiguration.
3. Wählen Sie auf der Registerkarte Organisation das Zielkonto oder die Organisationseinheit aus. Wählen Sie Bearbeiten aus.
4. Wählen Sie auf der Seite Konfiguration definieren als Verwaltungstyp die Option Zentral verwaltet aus, wenn der delegierte Administrator das Zielkonto oder die Organisationseinheit konfigurieren soll. Wählen Sie dann „Spezifische Richtlinie anwenden“ aus, wenn Sie dem Ziel eine bestehende Konfigurationsrichtlinie zuordnen möchten. Wählen Sie Von meiner Organisation übernehmen, wenn Sie möchten, dass das Ziel die Konfiguration seines engsten übergeordneten Unternehmens erbt. Wählen Sie aus, Self-managedob das Konto oder die Organisationseinheit ihre eigenen Einstellungen konfigurieren soll.
5. Wählen Sie Weiter aus. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern.

Security Hub CSPM API

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `ConfigurationPolicyIdentifier` Feld an, `SELF_MANAGED_SECURITY_HUB` ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.

3. Geben Sie für das `Target` Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispiel für eine API-Anfrage zur Benennung eines selbstverwalteten Kontos:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie `configuration-policy-identifier` im Feld an, `SELF_MANAGED_SECURITY_HUB` ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.
3. Geben Sie für das `target` Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispielbefehl zur Benennung eines selbstverwalteten Kontos:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

So funktionieren Konfigurationsrichtlinien in Security Hub CSPM

Der delegierte AWS Security Hub CSPM-Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für eine Organisation zu konfigurieren. Nach der Erstellung einer Konfigurationsrichtlinie kann der delegierte Administrator sie bestimmten Konten, Organisationseinheiten (OUs) oder dem Stamm zuordnen. Die Richtlinie wird dann für die angegebenen Konten, Organisationseinheiten oder das Stammverzeichnis wirksam.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Dieser Abschnitt bietet einen detaillierten Überblick über die Konfigurationsrichtlinien.

Überlegungen zu Richtlinien

Bevor Sie eine Konfigurationsrichtlinie in Security Hub CSPM erstellen, sollten Sie die folgenden Details berücksichtigen.

- Konfigurationsrichtlinien müssen verknüpft werden, damit sie wirksam werden. Nachdem Sie eine Konfigurationsrichtlinie erstellt haben, können Sie sie einem oder mehreren Konten, Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie kann Konten oder Organisationseinheiten durch direkte Anwendung oder durch Vererbung von einer übergeordneten Organisationseinheit zugeordnet werden.
- Ein Konto oder eine Organisationseinheit kann nur einer Konfigurationsrichtlinie zugeordnet werden. Um widersprüchliche Einstellungen zu vermeiden, kann ein Konto oder eine Organisationseinheit jeweils nur einer Konfigurationsrichtlinie zugeordnet werden. Alternativ kann ein Konto oder eine Organisationseinheit selbst verwaltet werden.
- Die Konfigurationsrichtlinien sind vollständig — Die Konfigurationsrichtlinien bieten eine vollständige Spezifikation der Einstellungen. Beispielsweise kann ein Kinderkonto keine Einstellungen für einige Steuerelemente aus einer Richtlinie und Einstellungen für andere Steuerelemente aus einer anderen Richtlinie akzeptieren. Wenn Sie eine Richtlinie einem Kinderkonto zuordnen, stellen Sie sicher, dass die Richtlinie alle Einstellungen festlegt, die das Kinderkonto verwenden soll.
- Konfigurationsrichtlinien können nicht rückgängig gemacht werden — Es gibt keine Möglichkeit, eine Konfigurationsrichtlinie rückgängig zu machen, nachdem Sie sie Konten oder Organisationseinheiten zugeordnet haben. Wenn Sie beispielsweise eine Konfigurationsrichtlinie, die CloudWatch Steuerelemente deaktiviert, einem bestimmten Konto zuordnen und diese Richtlinie dann aufheben, sind die CloudWatch Steuerelemente in diesem Konto weiterhin

deaktiviert. Um die CloudWatch Kontrollen wieder zu aktivieren, können Sie das Konto einer neuen Richtlinie zuordnen, die die Kontrollen aktiviert. Alternativ können Sie das Konto in „Selbstverwaltung“ ändern und alle CloudWatch Steuerelemente im Konto aktivieren.

- Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen — Eine Konfigurationsrichtlinie wirkt sich auf alle zugehörigen Konten in der Heimatregion und auf alle verknüpften Regionen aus. Sie können keine Konfigurationsrichtlinie erstellen, die nur in einigen dieser Regionen wirksam ist und in anderen nicht. Eine Ausnahme bilden Steuerelemente, die globale Ressourcen verwenden. Security Hub CSPM deaktiviert automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen.

  Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor dort eine Konfigurationsrichtlinie wirksam wird. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Anweisungen zur Aktivierung von Opt-in-Regionen finden Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Regionen für AWS-Regionen Ihr AWS Konto verwendet werden können.

  Wenn Ihre Richtlinie eine Steuerung konfiguriert, die in der Heimatregion oder einer oder mehreren verknüpften Regionen nicht verfügbar ist, überspringt Security Hub CSPM die Kontrollkonfiguration in nicht verfügbaren Regionen, wendet die Konfiguration jedoch in Regionen an, in denen die Steuerung verfügbar ist. Ihnen fehlt der Versicherungsschutz für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

- Konfigurationsrichtlinien sind Ressourcen — Als Ressource hat eine Konfigurationsrichtlinie einen Amazon-Ressourcennamen (ARN) und eine Universally Unique Identifier (UUID). Der ARN verwendet das folgende Format:`arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*. Eine selbstverwaltete Konfiguration hat keinen ARN oder UUID. Der Bezeichner für eine selbstverwaltete Konfiguration lautet. `SELF_MANAGED_SECURITY_HUB`
- Multicloud-Standards werden in Konfigurationsrichtlinien nicht unterstützt — Konfigurationsrichtlinien können nur AWS Sicherheitsstandards und Kontrollen beinhalten. Multicloud-Standards wie CIS Azure Foundations Benchmark v4.0.0 und die zugehörigen Steuerelemente (z. B.`Azure.Storage.1`) können nicht in eine Konfigurationsrichtlinie aufgenommen werden. Wenn Sie einen Multi-Cloud-Standard-ARN oder eine Kontroll-ID in eine Konfigurationsrichtlinie aufnehmen, gibt die Anfrage eine `InvalidInputException` zurück. Um Multicloud-Standards zu aktivieren oder zu konfigurieren, verwenden Sie lokale Konfigurationsmechanismen direkt in der gewünschten Version. AWS-Konto

Arten von Konfigurationsrichtlinien

Jede Konfigurationsrichtlinie legt die folgenden Einstellungen fest:

- Aktivieren oder deaktivieren Sie Security Hub CSPM.
- Aktivieren Sie einen oder mehrere Sicherheitsstandards.
- Geben Sie an, welche Sicherheitskontrollen für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.
- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Zentrale Konfigurationsrichtlinien beinhalten keine AWS Config Rekordereinstellungen. Sie müssen die Aufzeichnung für die erforderlichen Ressourcen separat aktivieren AWS Config und aktivieren, damit Security Hub CSPM Kontrollergebnisse generieren kann. Weitere Informationen finden Sie unter Überlegungen vor der Aktivierung und Konfiguration AWS Config.

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.

Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unterSteuerungen, die globale Ressourcen verwenden.

Empfohlene Konfigurationsrichtlinie

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie in der Security Hub CSPM-Konsole erstellen, haben Sie die Möglichkeit, die von Security Hub CSPM empfohlene Richtlinie auszuwählen.

Die empfohlene Richtlinie aktiviert Security Hub CSPM, den Standard AWS Foundational Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Richtlinie gilt für Root-Benutzer (alle Konten und Organisationseinheiten, sowohl neue als auch bestehende). Nachdem Sie die empfohlene Richtlinie für Ihre Organisation erstellt haben, können Sie sie über das delegierte Administratorkonto ändern. Sie können beispielsweise zusätzliche Standards oder Kontrollen aktivieren oder bestimmte FSBP-Steuerelemente deaktivieren. Anweisungen zum Ändern einer Konfigurationsrichtlinie finden Sie unterAktualisierung der Konfigurationsrichtlinien.

Benutzerdefinierte Konfigurationsrichtlinie

Anstelle der empfohlenen Richtlinie kann der delegierte Administrator bis zu 20 benutzerdefinierte Konfigurationsrichtlinien erstellen. Sie können Ihrer gesamten Organisation eine einzelne benutzerdefinierte Richtlinie oder verschiedene benutzerdefinierte Richtlinien verschiedenen Konten und Organisationseinheiten zuordnen. Für eine benutzerdefinierte Konfigurationsrichtlinie geben Sie Ihre gewünschten Einstellungen an. Sie können beispielsweise eine benutzerdefinierte Richtlinie erstellen, die FSBP, den Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 und alle Kontrollen in diesen Standards außer Amazon Redshift Redshift-Steuerelementen aktiviert. Der Grad der Granularität, den Sie in benutzerdefinierten Konfigurationsrichtlinien verwenden, hängt vom beabsichtigten Umfang der Sicherheitsabdeckung in Ihrem Unternehmen ab.

> **Note**
>
> Sie können dem delegierten Administratorkonto keine Konfigurationsrichtlinie zuordnen, die Security Hub CSPM deaktiviert. Eine solche Richtlinie kann mit anderen Konten verknüpft werden, überspringt jedoch die Zuordnung zum delegierten Administrator. Das delegierte Administratorkonto behält seine aktuelle Konfiguration bei.

Nachdem Sie eine benutzerdefinierte Konfigurationsrichtlinie erstellt haben, können Sie zur empfohlenen Konfigurationsrichtlinie wechseln, indem Sie Ihre Konfigurationsrichtlinie so aktualisieren, dass sie der empfohlenen Konfiguration entspricht. Sie sehen jedoch nicht die Möglichkeit, die empfohlene Konfigurationsrichtlinie in der Security Hub CSPM-Konsole zu erstellen, nachdem Ihre erste Richtlinie erstellt wurde.

Richtlinienverknüpfung durch Anwendung und Vererbung

Wenn Sie sich zum ersten Mal für die zentrale Konfiguration entscheiden, hat Ihre Organisation keine Zuordnungen und verhält sich genauso wie vor der Anmeldung. Der delegierte Administrator kann dann Verknüpfungen zwischen einer Konfigurationsrichtlinie oder einem selbstverwalteten Verhalten und Konten, Organisationseinheiten oder dem Stammverzeichnis herstellen. Verknüpfungen können durch Anwendung oder Vererbung hergestellt werden.

Über das delegierte Administratorkonto können Sie eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder das Stammkonto anwenden. Alternativ kann der delegierte Administrator einem Konto, einer Organisationseinheit oder dem Stammkonto direkt eine selbstverwaltete Bezeichnung zuweisen.

In Ermangelung einer direkten Anwendung erbt ein Konto oder eine Organisationseinheit die Einstellungen der nächstgelegenen übergeordneten Organisation, die über eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten verfügt. Wenn das engste Elternteil mit einer Konfigurationsrichtlinie verknüpft ist, erbt das Kind diese Richtlinie und kann nur vom delegierten Administrator aus der Heimatregion konfiguriert werden. Wenn der nächstgelegene Elternteil selbst verwaltet wird, erbt das Kind das selbstverwaltete Verhalten und kann in jedem Fall seine eigenen Einstellungen angeben. AWS-Region

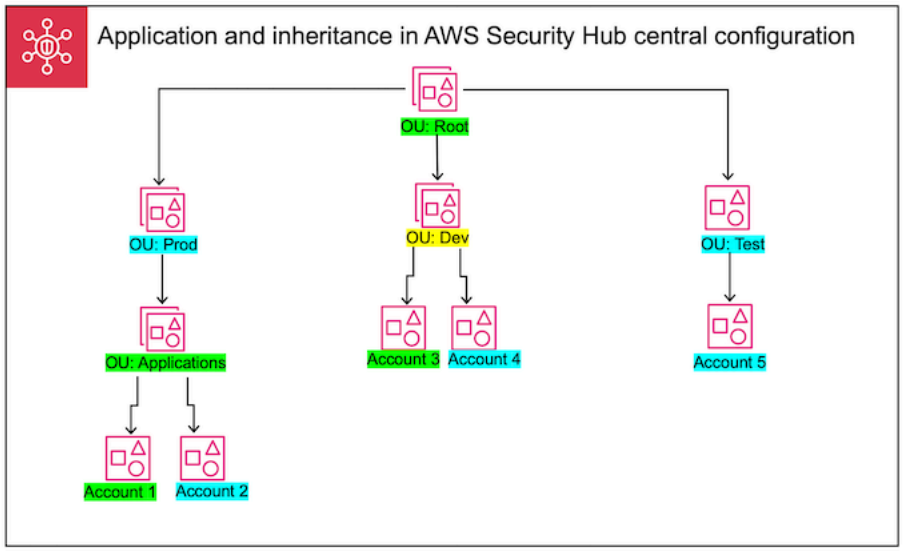
Die Anwendung hat Vorrang vor der Vererbung. Mit anderen Worten, die Vererbung setzt eine Konfigurationsrichtlinie oder eine selbstverwaltete Zuweisung, die der delegierte Administrator direkt auf ein Konto oder eine Organisationseinheit angewendet hat, nicht außer Kraft.

Wenn Sie eine Konfigurationsrichtlinie direkt auf ein selbstverwaltetes Konto anwenden, hat die Richtlinie Vorrang vor der Bezeichnung für selbstverwaltete Konten. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Wir empfehlen, eine Konfigurationsrichtlinie direkt auf das Stammverzeichnis anzuwenden. Wenn Sie eine Richtlinie auf das Stammverzeichnis anwenden, erben neue Konten, die Ihrer Organisation beitreten, automatisch die Stammrichtlinie, sofern Sie sie nicht einer anderen Richtlinie zuordnen oder sie als selbstverwaltet kennzeichnen.

Einem Konto oder einer Organisationseinheit kann jeweils nur eine Konfigurationsrichtlinie zugeordnet werden, entweder durch Anwendung oder Vererbung. Dadurch sollen widersprüchliche Einstellungen vermieden werden.

Das folgende Diagramm zeigt, wie die Anwendung und Vererbung von Richtlinien in einer zentralen Konfiguration funktionieren.



In diesem Beispiel wurde auf einen grün hervorgehobenen Knoten eine Konfigurationsrichtlinie angewendet. Auf einen blau hervorgehobenen Knoten wurde keine Konfigurationsrichtlinie angewendet. Ein gelb hervorgehobener Knoten wurde als selbstverwaltet eingestuft. Jedes Konto und jede Organisationseinheit verwendet die folgende Konfiguration:

- OU:Root (Grün) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- OU:Prod (Blau) — Diese Organisationseinheit erbt die Konfigurationsrichtlinie von OU:Root.
- OU:Applications (Grün) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- Konto 1 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 2 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von OU:Applications.
- OU:Dev (Gelb) — Diese Organisationseinheit wird selbst verwaltet.
- Konto 3 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 4 (Blau) — Dieses Konto erbt das selbstverwaltete Verhalten von. OU:Dev
- OU:Test (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von. OU:Root
- Konto 5 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von, OU:Root da das unmittelbar übergeordnete Konto OU:Test, keiner Konfigurationsrichtlinie zugeordnet ist.

Testen einer Konfigurationsrichtlinie

Um sicherzustellen, dass Sie verstehen, wie Konfigurationsrichtlinien funktionieren, empfehlen wir, eine Richtlinie zu erstellen und sie einem Testkonto oder einer Organisationseinheit zuzuordnen.

Um eine Konfigurationsrichtlinie zu testen

1. Erstellen Sie eine benutzerdefinierte Konfigurationsrichtlinie und stellen Sie sicher, dass die angegebenen Einstellungen für die Aktivierung, Standards und Kontrollen von Security Hub CSPM korrekt sind. Detaillierte Anweisungen finden Sie unter Konfigurationsrichtlinien erstellen und zuordnen.
2. Wenden Sie die Konfigurationsrichtlinie auf ein Testkonto oder eine Organisationseinheit an, die keine untergeordneten Konten oder Organisationseinheiten hat.
3. Stellen Sie sicher, dass das Testkonto oder die Organisationseinheit die Konfigurationsrichtlinie in Ihrer Heimatregion und allen verknüpften Regionen erwartungsgemäß verwendet. Sie können auch überprüfen, ob alle anderen Konten und Organisationseinheiten in Ihrer Organisation weiterhin selbst verwaltet werden und dass sie in jeder Region ihre eigenen Einstellungen ändern können.

Nachdem Sie eine Konfigurationsrichtlinie in einem einzelnen Konto oder einer einzelnen Organisationseinheit getestet haben, können Sie sie mit anderen Konten und Organisationseinheiten verknüpfen.

Konfigurationsrichtlinien erstellen und zuordnen

Das delegierte AWS Security Hub CSPM-Administratorkonto kann Konfigurationsrichtlinien erstellen, die festlegen, wie Security Hub CSPM, Standards und Kontrollen in bestimmten Konten und Organisationseinheiten (OUs) konfiguriert werden. Eine Konfigurationsrichtlinie wird erst wirksam, wenn der delegierte Administrator sie mindestens einem Konto oder einer Organisationseinheit (OUs) oder dem Stamm zuordnet. Der delegierte Administrator kann eine selbstverwaltete Konfiguration auch Konten, Organisationseinheiten oder dem Stammverzeichnis zuordnen.

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, empfehlen wir, diese zuerst zu überprüfen. So funktionieren Konfigurationsrichtlinien in Security Hub CSPM

> **Note**
>
> Konfigurationsrichtlinien unterstützen nur AWS Standards und Kontrollen. Sie können keine Multicloud-Standards (wie CIS Azure Foundations Benchmark v4.0.0) oder Azure-

Steuerelemente in eine Konfigurationsrichtlinie aufnehmen. Einschließlich einer Multi-Cloud-Standard-ARN- oder Kontroll-ID-Rückgabe`InvalidInputException`. Verwenden Sie lokale Konfigurationsmechanismen direkt im gewünschten Bereich, um Multicloud-Standards zu aktivieren oder zu konfigurieren. AWS-Konto

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten zum Erstellen und Zuordnen einer Konfigurationsrichtlinie oder einer selbstverwalteten Konfiguration. Wenn Sie die Security Hub CSPM-Konsole verwenden, können Sie eine Konfiguration mehreren Konten oder OUs gleichzeitig zuordnen. Wenn Sie die Security Hub CSPM API oder verwenden AWS CLI, können Sie in jeder Anfrage nur einem Konto oder einer Organisationseinheit eine Konfiguration zuordnen.

Note

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.
Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.
Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unter[Steuerungen, die globale Ressourcen verwenden](#).

Security Hub CSPM console

So erstellen Sie Konfigurationsrichtlinien und ordnen sie zu

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Konfiguration und dann die Registerkarte Richtlinien aus. Wählen Sie dann Richtlinie erstellen aus.
3. Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, werden auf der Seite Organisation konfigurieren unter Konfigurationstyp drei Optionen angezeigt. Wenn Sie bereits mindestens eine Konfigurationsrichtlinie erstellt haben, wird nur die Option Benutzerdefinierte Richtlinie angezeigt.

   - Wählen Sie Die AWS empfohlene Security Hub CSPM-Konfiguration für mein gesamtes Unternehmen verwenden, um unsere empfohlene Richtlinie zu verwenden. Die empfohlene Richtlinie aktiviert Security Hub CSPM in allen Unternehmenskonten, aktiviert den Standard AWS Foundational Security Best Practices (FSBP) und aktiviert alle neuen und vorhandenen FSBP-Steuerelemente. Die Steuerelemente verwenden Standardparameterwerte.
   - Wählen Sie Ich bin noch nicht bereit zur Konfiguration, um später eine Konfigurationsrichtlinie zu erstellen.
   - Wählen Sie Benutzerdefinierte Richtlinie, um eine benutzerdefinierte Konfigurationsrichtlinie zu erstellen. Geben Sie an, ob Security Hub CSPM aktiviert oder deaktiviert werden soll, welche Standards aktiviert werden sollen und welche Kontrollen für diese Standards aktiviert werden sollen. Geben Sie optional benutzerdefinierte Parameterwerte für ein oder mehrere aktivierte Steuerelemente an, die benutzerdefinierte Parameter unterstützen.
4. Wählen Sie im Abschnitt Konten aus, für welche Zielkonten, Organisationseinheiten oder das Stammkonto Ihre Konfigurationsrichtlinie gelten soll.

   - Wählen Sie Alle Konten aus, wenn Sie die Konfigurationsrichtlinie auf das Stammkonto anwenden möchten. Dies schließt alle Konten und Organisationseinheiten in der Organisation ein, auf die keine andere Richtlinie angewendet oder vererbt wurde.
   - Wählen Sie Bestimmte Konten aus, wenn Sie die Konfigurationsrichtlinie auf bestimmte Konten oder Organisationseinheiten anwenden möchten. Geben Sie die Konto-IDs ein, oder wählen Sie die Konten und Organisationseinheiten aus der Organisationsstruktur aus. Sie können die Richtlinie bei der Erstellung auf maximal 15 Ziele (Konten, OUs oder Root) anwenden. Um eine größere Zahl anzugeben, bearbeiten Sie Ihre Richtlinie nach der Erstellung und wenden Sie sie auf weitere Ziele an.

- Wählen Sie Nur der delegierte Administrator, um die Konfigurationsrichtlinie auf das aktuelle delegierte Administratorkonto anzuwenden.

5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Überprüfen und Anwenden die Details Ihrer Konfigurationsrichtlinie. Wählen Sie dann Richtlinie erstellen und anwenden aus. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit der Konfigurationsrichtlinie verknüpft werden. Untergeordnete Konten und Organisationseinheiten der angewendeten Ziele übernehmen automatisch diese Konfigurationsrichtlinie, sofern sie nicht ausdrücklich ausgeschlossen wurden, sie selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Security Hub CSPM API

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Rufen Sie die CreateConfigurationPolicyAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für `Name` einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für `Description` eine Beschreibung der Konfigurationsrichtlinie an.
3. Geben Sie für das `ServiceEnabled` Feld an, ob Security Hub CSPM in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das `EnabledStandardIdentifiers` Feld an, welche Security Hub CSPM-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das `SecurityControlsConfiguration` Objekt an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen Sie `EnabledSecurityControlIdentifiers` aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie `DisabledSecurityControlIdentifiers` diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.
6. Geben Sie optional für das `SecurityControlCustomParameters` Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie `CUSTOM` das

`ValueType` Feld und den benutzerdefinierten Parameterwert für das `Value` Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub CSPM angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter Grundlegendes zu den Steuerungsparametern in Security Hub CSPM.

7. Um Ihre Konfigurationsrichtlinie auf Konten oder Organisationseinheiten anzuwenden, rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
8. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den Amazon-Ressourcennamen (ARN) oder die Universally Unique Identifier (UUID) der Richtlinie ein. Der ARN und die UUID werden von der `CreateConfigurationPolicy` API zurückgegeben. Bei einer selbstverwalteten Konfiguration entspricht das `ConfigurationPolicyIdentifier` Feld. `SELF_MANAGED_SECURITY_HUB`
9. Geben Sie für das `Target` Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können in jeder API-Anfrage nur ein Ziel angeben. Untergeordnete Konten und Organisationseinheiten des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispiel für eine API-Anfrage zur Erstellung einer Konfigurationsrichtlinie:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
```

```
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Beispiel für eine API-Anfrage zum Zuordnen einer Konfigurationsrichtlinie:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Führen Sie den create-configuration-policyBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie für `name` einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für `description` eine Beschreibung der Konfigurationsrichtlinie an.
3. Geben Sie für das `ServiceEnabled` Feld an, ob Security Hub CSPM in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das `EnabledStandardIdentifiers` Feld an, welche Security Hub CSPM-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das `SecurityControlsConfiguration` Feld an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen

Sie `EnabledSecurityControlIdentifiers` aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie `DisabledSecurityControlIdentifiers` diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Ihren aktivierten Standards entsprechen (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.

6. Geben Sie optional für das `SecurityControlCustomParameters` Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie `CUSTOM` das `ValueType` Feld und den benutzerdefinierten Parameterwert für das `Value` Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub CSPM angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter Grundlegendes zu den Steuerungsparametern in Security Hub CSPM.
7. Um Ihre Konfigurationsrichtlinie auf Konten oder Organisationseinheiten anzuwenden, führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
8. Geben Sie für das `configuration-policy-identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein. Dieser ARN und diese ID werden vom `create-configuration-policy` Befehl zurückgegeben.
9. Geben Sie für das `target` Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können jedes Mal, wenn Sie den Befehl ausführen, nur ein Ziel angeben. Untergeordnete Objekte des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispielbefehl zum Erstellen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Beispielbefehl zum Zuordnen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens zurück`AssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unterÜberprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie.

Status und Details der Konfigurationsrichtlinien überprüfen

Der delegierte AWS Security Hub CSPM-Administrator kann die Konfigurationsrichtlinien für eine Organisation und deren Details einsehen. Dazu gehört, mit welchen Konten und Organisationseinheiten (OUs) eine Richtlinie verknüpft ist.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre Konfigurationsrichtlinien einzusehen.

Security Hub CSPM console

So zeigen Sie die Konfigurationsrichtlinien an (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.

3. Wählen Sie die Registerkarte Richtlinien, um einen Überblick über Ihre Konfigurationsrichtlinien zu erhalten.
4. Wählen Sie eine Konfigurationsrichtlinie aus und klicken Sie auf Details anzeigen, um weitere Informationen zu dieser Richtlinie anzuzeigen, einschließlich der Konten und Organisationseinheiten, mit denen sie verknüpft ist.

Security Hub CSPM API

Um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien anzuzeigen, verwenden Sie den ListConfigurationPoliciesBetrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den list-configuration-policiesBefehl aus. Das delegierte Security Hub CSPM-Administratorkonto sollte den Vorgang in der Heimatregion aufrufen.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Verwenden Sie den Vorgang, um Details zu einer bestimmten Konfigurationsrichtlinie anzuzeigen. GetConfigurationPolicy Wenn Sie den verwendenAWS CLI, führen Sie den aus get-configuration-policy. Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, deren Details Sie sehen möchten.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Verwenden Sie den ListConfigurationPolicyAssociationsVorgang, um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien und ihrer Kontozuordnungen anzuzeigen. Wenn Sie den verwendenAWS CLI, führen Sie den list-configuration-policy-associationsBefehl aus. Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Optional können Sie Paginierungsparameter angeben oder die Ergebnisse nach einer bestimmten Richtlinien-ID, einem Zuordnungstyp oder einem Zuordnungsstatus filtern.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Verwenden Sie den GetConfigurationPolicyAssociationVorgang, um Verknüpfungen für ein bestimmtes Konto anzuzeigen. Wenn Sie den verwendenAWS CLI, führen Sie den get-configuration-policy-associationBefehl aus. Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Geben Sie für `target` die Kontonummer, OU-ID oder Root-ID an.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Überprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie

Die folgenden API-Operationen für die zentrale Konfiguration geben ein Feld mit dem Namen zurück`AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Dieses Feld wird sowohl zurückgegeben, wenn es sich bei der zugrunde liegenden Konfiguration um eine Konfigurationsrichtlinie handelt, als auch wenn es sich um ein selbstverwaltetes Verhalten handelt.

Der Wert von `AssociationStatus` gibt an, ob eine Richtlinienzuweisung für ein bestimmtes Konto noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILED`. Ein Status von `SUCCESS` bedeutet, dass alle in der Konfigurationsrichtlinie angegebenen Einstellungen dem Konto zugeordnet sind. Ein Status von `FAILED` bedeutet, dass eine oder mehrere in der Konfigurationsrichtlinie angegebene Einstellungen dem Konto nicht zugeordnet werden konnten. Trotz eines `FAILED` Status konnte das Konto gemäß der Richtlinie teilweise konfiguriert werden. Sie könnten beispielsweise versuchen, ein Konto mit einer Konfigurationsrichtlinie zu verknüpfen, die Security Hub CSPM aktiviert, AWS Foundational Security Best Practices aktiviert und deaktiviert. CloudTrail.1 Die ersten beiden Einstellungen könnten erfolgreich sein, aber die CloudTrail.1 Einstellung könnte fehlschlagen. In diesem Beispiel lautet der Zuordnungsstatus, `FAILED` obwohl einige Einstellungen korrekt konfiguriert wurden.

Der Zuordnungsstatus einer übergeordneten Organisationseinheit oder der Stammorganisation hängt vom Status ihrer untergeordneten Organisationseinheiten ab. Wenn der Assoziationsstatus

aller Kinder lautet`SUCCESS`, ist der Assoziationsstatus des Elternteils`SUCCESS`. Wenn der Assoziationsstatus eines oder mehrerer Kinder lautet`FAILED`, ist der Assoziationsstatus des Elternteils`FAILED`.

Der Wert von `AssociationStatus` hängt vom Assoziationsstatus der Police in allen relevanten Regionen ab. Wenn die Assoziation in der Heimatregion und allen verbundenen Regionen erfolgreich ist, `AssociationStatus` ist `SUCCESS` der Wert von. Wenn die Zuordnung in einer oder mehreren dieser Regionen fehlschlägt, `AssociationStatus` ist `FAILED` der Wert von.

Das folgende Verhalten wirkt sich auch auf den Wert von aus`AssociationStatus`:

- Handelt es sich bei dem Ziel um eine übergeordnete Organisationseinheit oder um die Stammorganisation, hat sie nur dann den `AssociationStatus` Wert „Ein“ `SUCCESS` oder „`FAILED`nur“, wenn alle untergeordneten Organisationseinheiten den `FAILED` Status „`SUCCESS`Oder“ haben. Wenn sich der Zuordnungsstatus eines untergeordneten Kontos oder einer Organisationseinheit ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie das übergeordnete Konto mit einer Konfiguration verknüpft haben, wird durch die Änderung der Zuordnungsstatus des übergeordneten Kontos nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.
- Handelt es sich bei dem Ziel um ein Konto, hat es den `AssociationStatus` Wert „Von“ `SUCCESS` oder `FAILED` nur, wenn die Zuordnung ein Ergebnis von `SUCCESS` oder `FAILED` in der Heimatregion und allen verknüpften Regionen hat. Wenn sich der Zuordnungsstatus eines Zielkontos ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie es zum ersten Mal mit einer Konfiguration verknüpft haben, wird sein Zuordnungsstatus aktualisiert. Durch die Änderung wird der Zuordnungsstatus des übergeordneten Elements jedoch nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.

Wenn Sie eine neue verknüpfte Region hinzufügen, repliziert Security Hub CSPM Ihre vorhandenen Verknüpfungen, die sich in einem `PENDING``SUCCESS`, oder `FAILED` Bundesstaat der neuen Region befinden.

Selbst wenn der Zuordnungsstatus lautet`SUCCESS`, kann der Aktivierungsstatus eines Standards, der Teil der Richtlinie ist, in einen unvollständigen Status übergehen. In diesem Fall kann Security Hub CSPM keine Ergebnisse für die Kontrollen des Standards generieren. Weitere Informationen finden Sie unter Den Status eines Standards überprüfen.

Behebung eines Zuordnungsfehlers

In AWS Security Hub CSPM kann eine Zuordnung von Konfigurationsrichtlinien aus den folgenden häufigen Gründen fehlschlagen.

- Das Organisationsverwaltungskonto ist kein Mitglied — Wenn Sie dem Organisationsverwaltungskonto eine Konfigurationsrichtlinie zuordnen möchten, muss AWS Security Hub CSPM für dieses Konto bereits aktiviert sein. Dadurch wird das Verwaltungskonto zu einem Mitgliedskonto in der Organisation.
- AWS Configist nicht aktiviert oder nicht richtig konfiguriert — Um Standards in einer Konfigurationsrichtlinie zu aktivieren, AWS Config muss sie aktiviert und konfiguriert sein, um relevante Ressourcen aufzuzeichnen.
- Muss über ein delegiertes Administratorkonto verknüpft werden — Sie können eine Richtlinie nur Zielkonten und Organisationseinheiten zuordnen, wenn Sie mit dem delegierten Security Hub CSPM-Administratorkonto angemeldet sind.
- Verbindung muss von der Heimatregion aus erfolgen — Sie können eine Richtlinie nur Zielkonten und Organisationseinheiten zuordnen, wenn Sie in Ihrer Heimatregion angemeldet sind.
- Opt-in Region nicht aktiviert — Die Richtlinienzuweisung schlägt für ein Mitgliedskonto oder eine Organisationseinheit in einer verknüpften Region fehl, wenn es sich um eine Opt-in-Region handelt, die der delegierte Administrator nicht aktiviert hat. Sie können es erneut versuchen, nachdem Sie die Region über das delegierte Administratorkonto aktiviert haben.
- Mitgliedskonto gesperrt — Die Richtlinienverknüpfung schlägt fehl, wenn Sie versuchen, eine Richtlinie mit einem gesperrten Mitgliedskonto zu verknüpfen.

Aktualisierung der Konfigurationsrichtlinien

Nach der Erstellung einer Konfigurationsrichtlinie kann das delegierte AWS Security Hub CSPM-Administratorkonto die Richtliniendetails und Richtlinienzuordnungen aktualisieren. Wenn die Richtliniendetails aktualisiert werden, verwenden Konten, die der Konfigurationsrichtlinie zugeordnet sind, automatisch die aktualisierte Richtlinie.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

> **Note**
>
> Konfigurationsrichtlinien unterstützen nur AWS Standards und Kontrollen. Sie können keine Multicloud-Standards (wie CIS Azure Foundations Benchmark v4.0.0) oder Azure-Steuerelemente in eine Konfigurationsrichtlinie aufnehmen. Einschließlich einer Multi-Cloud-Standard-ARN- oder Kontroll-ID-Rückgabe`InvalidInputException`. Verwenden Sie lokale Konfigurationsmechanismen direkt in der gewünschten Version, um Multicloud-Standards zu aktivieren oder zu konfigurieren. AWS-Konto

Der delegierte Administrator kann die folgenden Richtlinieneinstellungen aktualisieren:

- Aktivieren oder deaktivieren Sie Security Hub CSPM.
- Aktivieren Sie einen oder mehrere Sicherheitsstandards.
- Geben Sie an, welche Sicherheitskontrollen für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.
- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Aktualisieren einer Konfigurationsrichtlinie.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.
> Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften

Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.
Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unterSteuerungen, die globale Ressourcen verwenden.

Console

So aktualisieren Sie die Konfigurationsrichtlinien

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie die Konfigurationsrichtlinie aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus. Falls gewünscht, bearbeiten Sie die Richtlinieneinstellungen. Lassen Sie diesen Abschnitt unverändert, wenn Sie die Richtlinieneinstellungen unverändert lassen möchten.
5. Wählen Sie Weiter. Falls gewünscht, bearbeiten Sie die Richtlinienverknüpfungen. Lassen Sie diesen Abschnitt unverändert, wenn Sie die Richtlinienverknüpfungen unverändert lassen möchten. Sie können die Richtlinie bei der Aktualisierung maximal 15 Zielen (Konten, Organisationseinheiten oder Root) zuordnen oder deren Zuordnung aufheben.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern und anwenden. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit einer Konfigurationsrichtlinie verknüpft werden.

API

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, rufen Sie die UpdateConfigurationPolicyAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter ein`ConfigurationPolicy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, rufen Sie die StartConfigurationPolicyDisassociationAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
5. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `Target` Feld die Konten, Organisationseinheiten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen Organisationseinheiten oder Konten außer Kraft.

> **Note**
>
> Wenn Sie die `UpdateConfigurationPolicy` API aufrufen, führt Security Hub CSPM eine vollständige Listenersetzung für die Felder`EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, und durch. `SecurityControlCustomParameters` Geben Sie bei jedem Aufruf dieser API die vollständige Liste der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren möchten, und für die Sie die Parameter anpassen möchten.

Beispiel für eine API-Anfrage zur Aktualisierung einer Konfigurationsrichtlinie:

```
{
```

```
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, führen Sie den update-configuration-policyBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter ein`configuration-policy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, führen Sie den start-configuration-policy-disassociationBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
5. Geben Sie für das `configuration-policy-identifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `target` Feld die Konten, Organisationseinheiten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen Organisationseinheiten oder Konten außer Kraft.

> **Note**
>
> Wenn Sie den `update-configuration-policy` Befehl ausführen, führt Security Hub CSPM eine vollständige Listenersetzung für die Felder`EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, und `SecurityControlCustomParameters` durch. Geben Sie bei jeder Ausführung dieses Befehls die vollständige Liste der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren möchten, und für die Sie die Parameter anpassen möchten.

Beispielbefehl zum Aktualisieren einer Konfigurationsrichtlinie:

```
aws securityhub update-configuration-policy \
```

```
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens zurück`AssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unterÜberprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie.

Löschen von Konfigurationsrichtlinien

Nach der Erstellung einer Konfigurationsrichtlinie kann der delegierte AWS Security Hub CSPM-Administrator sie löschen. Alternativ kann der delegierte Administrator die Richtlinie beibehalten, sie jedoch von bestimmten Konten oder Organisationseinheiten (OUs) oder vom Stammverzeichnis trennen. Anweisungen zum Aufheben der Zuordnung zu einer Richtlinie finden Sie unter. Eine Konfiguration von ihren Zielen trennen

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter. Grundlegendes zur zentralen Konfiguration in Security Hub CSPM

In diesem Abschnitt wird erklärt, wie Konfigurationsrichtlinien gelöscht werden.

Wenn Sie eine Konfigurationsrichtlinie löschen, ist sie für Ihre Organisation nicht mehr vorhanden. Zielkonten, Organisationseinheiten und das Stammverzeichnis der Organisation können die Konfigurationsrichtlinie nicht mehr verwenden. Ziele, die mit einer gelöschten Konfigurationsrichtlinie verknüpft waren, erben die Konfigurationsrichtlinie des nächstgelegenen übergeordneten Objekts oder werden selbst verwaltet, wenn das nächstgelegene übergeordnete Objekt selbst verwaltet wird. Wenn Sie möchten, dass ein Ziel eine andere Konfiguration verwendet, können Sie das

Ziel einer neuen Konfigurationsrichtlinie zuordnen. Weitere Informationen finden Sie unter Konfigurationsrichtlinien erstellen und zuordnen.

Wir empfehlen, mindestens eine Konfigurationsrichtlinie zu erstellen und mit Ihrer Organisation zu verknüpfen, um einen angemessenen Sicherheitsschutz zu gewährleisten.

Bevor Sie eine Konfigurationsrichtlinie löschen können, müssen Sie die Zuordnung der Richtlinie zu allen Konten, Organisationseinheiten oder dem Stamm aufheben, für die sie derzeit gilt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen einer Konfigurationsrichtlinie.

Console

So löschen Sie eine Konfigurationsrichtlinie

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies. Wählen Sie die Konfigurationsrichtlinie aus, die Sie löschen möchten, und wählen Sie Löschen aus. Wenn die Konfigurationsrichtlinie noch mit Konten oder Organisationseinheiten verknüpft ist, werden Sie aufgefordert, die Richtlinie zunächst von diesen Zielen zu trennen, bevor Sie sie löschen können.
4. Überprüfen Sie die Bestätigungsnachricht. Geben Sie ein **`confirm`** und wählen Sie Löschen.

API

So löschen Sie eine Konfigurationsrichtlinie

Rufen Sie die DeleteConfigurationPolicyAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder Organisationseinheiten in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder Organisationseinheiten, bevor Sie versuchen, sie zu löschen.

Beispiel für eine API-Anfrage zum Löschen einer Konfigurationsrichtlinie:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

So löschen Sie eine Konfigurationsrichtlinie

Führen Sie den delete-configuration-policyBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder Organisationseinheiten in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder Organisationseinheiten, bevor Sie versuchen, sie zu löschen.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Eine Konfiguration von ihren Zielen trennen

Über das delegierte AWS Security Hub CSPM-Administratorkonto können Sie die Zuordnung einer Konfigurationsrichtlinie oder einer selbstverwalteten Konfiguration zu einem Konto, einer Organisationseinheit oder einem Root-Konto aufheben. Durch die Trennung der Zuordnung wird die Richtlinie für die future Verwendung beibehalten, bestehende Verknüpfungen zu bestimmten Konten, Organisationseinheiten oder dem Stammverzeichnis werden jedoch entfernt. Sie können nur eine direkt angewendete Konfiguration trennen, keine vererbte Konfiguration. Um eine geerbte Konfiguration zu ändern, können Sie eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten auf das betroffene Konto oder die betroffene Organisationseinheit anwenden. Sie können auch eine neue Konfigurationsrichtlinie, die Ihre gewünschten Änderungen enthält, auf das nächstgelegene übergeordnete Objekt anwenden.

Durch die Trennung der Zuordnung wird eine Konfigurationsrichtlinie nicht gelöscht. Die Richtlinie wird in Ihrem Konto gespeichert, sodass Sie sie mit anderen Zielen in Ihrer Organisation verknüpfen können. Anweisungen zum Löschen einer Konfigurationsrichtlinie finden Sie unterLöschen von Konfigurationsrichtlinien. Wenn die Trennung abgeschlossen ist, erbt ein betroffenes Ziel die Konfigurationsrichtlinie oder das selbstverwaltete Verhalten des nächstgelegenen übergeordneten Ziels. Wenn es keine vererbbare Konfiguration gibt, behält ein Ziel die Einstellungen bei, die es vor der Trennung hatte, wird aber selbst verwaltet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto, eine Organisationseinheit oder einen Root-Benutzer von der aktuellen Konfiguration zu trennen.

Console

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Organizations das Konto, die Organisationseinheit oder das Stammverzeichnis aus, das Sie von der aktuellen Konfiguration trennen möchten. Wählen Sie Bearbeiten aus.
4. Wählen Sie auf der Seite Konfiguration definieren für Verwaltung die Option Anwendete Richtlinie aus, wenn der delegierte Administrator Richtlinien direkt auf das Ziel anwenden kann. Wählen Sie Vererbt aus, wenn das Ziel die Konfiguration seines nächstgelegenen übergeordneten Objekts erben soll. In beiden Fällen kontrolliert der delegierte Administrator die Einstellungen für das Ziel. Wählen Sie aus, Self-managedob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll.
5. Nachdem Sie Ihre Änderungen überprüft haben, wählen Sie Weiter und Anwenden. Diese Aktion setzt bestehende Konfigurationen aller Konten oder Organisationseinheiten außer Kraft, die im Geltungsbereich enthalten sind, falls diese Konfigurationen mit Ihrer aktuellen Auswahl in Konflikt stehen.

API

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Rufen Sie die StartConfigurationPolicyDisassociationAPI über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für `ConfigurationPolicyIdentifier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `Target` die Konten, Organisationseinheiten oder den Stamm an, die Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispiel für eine API-Anfrage zum Trennen der Zuordnung zu einer Konfigurationsrichtlinie:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Führen Sie den start-configuration-policy-disassociationBefehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie für `configuration-policy-identifier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `target` die Konten, Organisationseinheiten oder den Stamm an, die Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispielbefehl zum Trennen der Zuordnung einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
```

```
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Konfiguration eines Standards oder einer Steuerung im Kontext

Wenn Sie die zentrale Konfiguration in AWS Security Hub CSPM verwenden, kann der delegierte Security Hub CSPM-Administrator Konfigurationsrichtlinien erstellen, die festlegen, wie Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für eine Organisation konfiguriert werden. Der delegierte Administrator kann Richtlinien bestimmten Konten und Organisationseinheiten (OU) zuordnen. Die Richtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen. Der delegierte Administrator kann die Konfigurationsrichtlinien bei Bedarf aktualisieren.

Auf der Security Hub CSPM-Konsole kann der delegierte Administrator die Konfigurationsrichtlinien auf zwei Arten aktualisieren: von der Konfigurationsseite aus oder im Kontext mit bestehenden Workflows. Letzteres kann von Vorteil sein, da Sie anhand der Sicherheitsergebnisse herausfinden können, welche Standards und Kontrollen für Ihre Umgebung am relevantesten sind, und diese gleichzeitig konfigurieren können.

In-context Die Konfiguration ist nur auf der Security Hub CSPM-Konsole verfügbar. Programmgesteuert muss der delegierte Administrator den UpdateConfigurationPolicyBetrieb der Security Hub CSPM-API aufrufen, um die Konfiguration bestimmter Standards oder Kontrollen in der Organisation zu ändern.

Gehen Sie wie folgt vor, um einen Security Hub CSPM-Standard oder eine kontextbezogene Steuerung zu konfigurieren.

So konfigurieren Sie einen Standard oder ein kontextbezogenes Steuerelement (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich eine der folgenden Optionen:

   - Um einen Standard zu konfigurieren, wählen Sie Sicherheitsstandards und dann einen bestimmten Standard aus.

- Um ein Steuerelement zu konfigurieren, wählen Sie Controls und wählen Sie ein bestimmtes Steuerelement aus.

3. Die Konsole listet Ihre vorhandenen Security Hub CSPM-Konfigurationsrichtlinien und den Status des ausgewählten Standards oder Steuerelements in jeder Richtlinie auf. Wählen Sie in jeder vorhandenen Konfigurationsrichtlinie die Optionen aus, um den Standard oder die Steuerung zu aktivieren oder zu deaktivieren. Bei Steuerungen können Sie auch die Steuerparameter anpassen. Sie können während der kontextbezogenen Konfiguration keine neue Richtlinie erstellen. Um eine neue Richtlinie zu erstellen, müssen Sie zur Konfigurationsseite gehen, die Registerkarte Richtlinien und dann Richtlinie erstellen auswählen.
4. Nachdem Sie Ihre Änderungen vorgenommen haben, wählen Sie Weiter.
5. Überprüfen Sie Ihre Änderungen und wählen Sie Anwenden. Die Updates wirken sich auf alle Konten und Organisationseinheiten aus, die einer geänderten Konfigurationsrichtlinie zugeordnet sind. Die Updates werden auch in der Heimatregion und allen verknüpften Regionen wirksam.

Deaktivierung der zentralen Konfiguration in Security Hub CSPM

Wenn Sie die zentrale Konfiguration in AWS Security Hub CSPM deaktivieren, verliert der delegierte Administrator die Möglichkeit, Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für mehrere Organisationseinheiten (OUs) zu konfigurierenAWS-Konten, und. AWS-Regionen Stattdessen müssen Sie die meisten Einstellungen für jedes Konto in jeder Region separat konfigurieren.

> **Important**
>
> Bevor Sie die zentrale Konfiguration deaktivieren können, müssen Sie zunächst Ihre Konten und Organisationseinheiten von ihrer aktuellen Konfiguration trennen, unabhängig davon, ob es sich dabei um eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten handelt. Bevor Sie die zentrale Konfiguration deaktivieren können, müssen Sie auch vorhandene Konfigurationsrichtlinien löschen.

Wenn Sie die zentrale Konfiguration deaktivieren, treten die folgenden Änderungen auf:

- Der delegierte Administrator kann keine Konfigurationsrichtlinien mehr für die Organisation erstellen.

- Konten, auf die eine Konfigurationsrichtlinie angewendet oder vererbt wurde, behalten ihre aktuellen Einstellungen bei, werden jedoch automatisch verwaltet.
- Ihr Unternehmen wechselt zur lokalen Konfiguration. Bei der lokalen Konfiguration müssen die meisten Security Hub CSPM-Einstellungen für jedes Organisationskonto und jede Region separat konfiguriert werden. Der delegierte Administrator kann festlegen, dass Security Hub CSPM, Standardsicherheitsstandards und alle Kontrollen, die Teil der Standardstandards sind, in neuen Organisationskonten automatisch aktiviert werden. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Diese Einstellungen sind nur in der aktuellen Region wirksam und wirken sich nur auf neue Unternehmenskonten aus. Der delegierte Administrator kann nicht ändern, welche Standards die Standardstandards sind. Die lokale Konfiguration unterstützt nicht die Verwendung von Konfigurationsrichtlinien oder Konfigurationen auf OU-Ebene.

Die Identität des delegierten Administratorkontos bleibt unverändert, wenn Sie die zentrale Konfiguration nicht mehr verwenden. Ihre Heimatregion und die verknüpften Regionen bleiben ebenfalls unverändert (Ihre Heimatregion wird jetzt als Aggregationsregion bezeichnet und kann für die Suche nach Aggregationen verwendet werden).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die zentrale Konfiguration nicht mehr zu verwenden und zur lokalen Konfiguration zu wechseln.

Security Hub CSPM console

Um die zentrale Konfiguration (Konsole) zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie im Abschnitt Übersicht die Option Bearbeiten aus.
4. Wählen Sie im Feld Organisationskonfiguration bearbeiten die Option Lokale Konfiguration aus. Falls Sie dies noch nicht getan haben, werden Sie aufgefordert, Ihre aktuellen Konfigurationsrichtlinien zu trennen und zu löschen, bevor Sie die zentrale Konfiguration beenden können. Konten oder Organisationseinheiten, die als selbstverwaltet gekennzeichnet sind, müssen von ihrer selbstverwalteten Konfiguration getrennt werden.

Sie können dies in der Konsole tun, indem Sie den Verwaltungstyp jedes selbstverwalteten Kontos oder jeder Organisationseinheit auf Zentral verwaltet und von meiner Organisation übernehmen ändern.

5. Wählen Sie optional die Standardeinstellungen für die lokale Konfiguration für neue Organisationskonten aus.
6. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Um die zentrale Konfiguration (API) zu deaktivieren

1. Rufen Sie die UpdateOrganizationConfigurationAPI auf.
2. Setzen Sie das `ConfigurationType` Feld im `OrganizationConfiguration` Objekt auf`LOCAL`. Die API gibt einen Fehler zurück, wenn Sie über bestehende Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Rufen Sie die API auf, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben. `StartConfigurationPolicyDisassociation` Rufen Sie die API auf, um eine Konfigurationsrichtlinie zu löschen. `DeleteConfigurationPolicy`
3. Wenn Sie Security Hub CSPM automatisch in neuen Organisationskonten aktivieren möchten, setzen Sie das `AutoEnable` Feld auf. `true` Standardmäßig ist der Wert dieses Feld`false`, und Security Hub CSPM wird nicht automatisch in neuen Organisationskonten aktiviert. Wenn Sie die Standardsicherheitsstandards für neue Organisationskonten automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld optional auf. `DEFAULT` Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld auf`NONE`.

Beispiel für eine API-Anfrage:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Um die zentrale Konfiguration zu deaktivieren (AWS CLI)

1. Führen Sie den Befehl update-organization-configuration aus.
2. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf ein`LOCAL`. Der Befehl gibt einen Fehler zurück, wenn Sie bereits über Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Führen Sie den `start-configuration-policy-disassociation` Befehl aus, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben. Führen Sie den `delete-configuration-policy` Befehl aus, um eine Konfigurationsrichtlinie zu löschen.
3. Wenn Sie Security Hub CSPM automatisch in neuen Organisationskonten aktivieren möchten, geben Sie den `auto-enable` Parameter an. Standardmäßig ist der Wert dieses Parameters`no-auto-enable`, und Security Hub CSPM wird nicht automatisch in neuen Organisationskonten aktiviert. Wenn Sie die Standardsicherheitsstandards für neue Organisationskonten automatisch aktivieren möchten, setzen Sie das `auto-enable-standards` Feld optional auf. `DEFAULT` Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `auto-enable-standards` Feld auf`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Verwaltung von Administrator- und Mitgliedskonten in Security Hub CSPM

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie die Konten, die AWS Security Hub CSPM verwenden, als Mitgliedskonten behandeln und sie einem einzigen Administratorkonto zuordnen. Der Administrator kann Ihren allgemeinen Sicherheitsstatus überwachen und zulässige Aktionen für Mitgliedskonten ergreifen. Der Administrator kann auch verschiedene Aufgaben zur Kontoverwaltung und -verwaltung in großem Umfang ausführen, z. B. die Überwachung der geschätzten Nutzungskosten und die Bewertung der Kontokontingente.

Sie können Mitgliedskonten auf zwei Arten einem Administrator zuordnen, indem Sie Security Hub CSPM in Security Hub CSPM integrieren AWS Organizations oder indem Sie Mitgliedschaftseinladungen manuell in Security Hub CSPM senden und annehmen.

Konten verwalten mitAWS Organizations

AWS Organizationsist ein globaler Kontoverwaltungsdienst, mit dem AWS Administratoren mehrere Konten konsolidieren und verwalten können. AWS-Konten Er bietet Funktionen zur Kontoverwaltung und konsolidierten Fakturierung, die auf die Erfüllung von Haushalts-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrierenAWS-Services, darunter AWS Security Hub CSPM, Amazon Macie und Amazon. GuardDuty Weitere Informationen finden Sie im AWS Organizations-Benutzerhandbuch.

Wenn Sie Security Hub CSPM und integrierenAWS Organizations, bestimmt das Verwaltungskonto der Organizations einen delegierten Security Hub CSPM-Administrator. Security Hub CSPM wird automatisch in dem delegierten Administratorkonto aktiviert, AWS-Region in dem es zugewiesen wurde.

Nach der Benennung eines delegierten Administrators empfehlen wir, Konten in Security Hub CSPM mit zentraler Konfiguration zu verwalten. Dies ist die effizienteste Methode, Security Hub CSPM individuell anzupassen und eine angemessene Sicherheitsabdeckung für Ihr Unternehmen sicherzustellen.

Durch die zentrale Konfiguration kann der delegierte Administrator Security Hub CSPM für mehrere Unternehmenskonten und Regionen anpassen, anstatt es zu konfigurieren. Region-by-Region Sie können eine Konfigurationsrichtlinie für Ihr gesamtes Unternehmen oder unterschiedliche Konfigurationsrichtlinien für verschiedene Konten und Organisationseinheiten erstellen. Die Richtlinien geben an, ob Security Hub CSPM in den zugehörigen Konten aktiviert oder deaktiviert ist und welche Sicherheitsstandards und Kontrollen aktiviert sind.

Der delegierte Administrator kann Konten als zentral verwaltete oder selbstverwaltete Konten festlegen. Zentral verwaltete Konten können nur vom delegierten Administrator konfiguriert werden. Self-managed Konten können ihre eigenen Einstellungen angeben.

Wenn Sie sich nicht für die zentrale Konfiguration entscheiden, hat der delegierte Administrator eine eingeschränktere Möglichkeit, Security Hub CSPM zu konfigurieren, was als lokale Konfiguration bezeichnet wird. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und Standardsicherheitsstandards automatisch in neuen Unternehmenskonten in der aktuellen

Region aktivieren. Bestehende Konten verwenden diese Einstellungen jedoch nicht, sodass es nach dem Beitritt eines Kontos zur Organisation zu Konfigurationsabweichungen kommen kann.

Abgesehen von diesen neuen Kontoeinstellungen ist die lokale Konfiguration kontospezifisch und. Region-specific Jedes Organisationskonto muss den Security Hub CSPM-Dienst, die Standards und Kontrollen in jeder Region separat konfigurieren. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Manuelles Verwalten von Konten auf Einladung

Sie müssen Mitgliedskonten auf Einladung manuell in Security Hub CSPM verwalten, wenn Sie ein eigenständiges Konto haben oder wenn Sie nicht in Organizations integriert sind. Ein eigenständiges Konto kann nicht in Organizations integriert werden, daher muss es manuell verwaltet werden. Wir empfehlen, die zentrale Konfiguration zu integrieren AWS Organizations und diese zu verwenden, wenn Sie in future weitere Konten hinzufügen.

Wenn Sie die manuelle Kontoverwaltung verwenden, bestimmen Sie ein Konto als Security Hub CSPM-Administrator. Das Administratorkonto kann Daten in Mitgliedskonten einsehen und bestimmte Maßnahmen ergreifen, wenn die Ergebnisse des Mitgliedskontos berücksichtigt werden. Der Security Hub CSPM-Administrator lädt andere Konten als Mitgliedskonten ein, und die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Ohne Konfigurationsrichtlinien kann der Administrator Security Hub CSPM nicht zentral anpassen, indem er variable Einstellungen für verschiedene Konten konfiguriert. Stattdessen muss jedes Organisationskonto Security Hub CSPM für sich selbst in jeder Region separat aktivieren und konfigurieren. Dies kann es schwieriger und zeitaufwändiger machen, eine angemessene Sicherheitsabdeckung für alle Konten und Regionen sicherzustellen, in denen Sie Security Hub CSPM verwenden. Dies kann auch zu Konfigurationsabweichungen führen, da Mitgliedskonten ihre eigenen Einstellungen ohne Eingaben des Administrators angeben können.

Informationen zur Verwaltung von Konten auf Einladung finden Sie unterKonten auf Einladung in Security Hub CSPM verwalten.

Empfehlungen für die Verwaltung mehrerer Konten in Security Hub CSPM

Im folgenden Abschnitt werden einige Einschränkungen und Empfehlungen zusammengefasst, die Sie bei der Verwaltung von Mitgliedskonten in AWS Security Hub CSPM beachten sollten.

Maximale Anzahl von Mitgliedern pro Konto

Wenn Sie die Integration mit verwendenAWS Organizations, unterstützt Security Hub CSPM jeweils bis zu 10.000 Mitgliedskonten pro delegiertem Administratorkonto. AWS-Region Wenn Sie Security Hub CSPM manuell aktivieren und verwalten, unterstützt Security Hub CSPM bis zu 1.000 Mitgliedskonteneinladungen pro Administratorkonto in jeder Region.

Beziehungen zwischen Administrator und Mitglied erstellen

> **Note**
>
> Wenn Sie die Security Hub CSPM-Integration mit AWS Organizations verwenden und keine Mitgliedskonten manuell eingeladen haben, gilt dieser Abschnitt nicht für Sie.

Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Ein Mitgliedskonto kann nur einem Administratorkonto zugeordnet werden. Wenn ein Organisationskonto durch das Security Hub CSPM-Administratorkonto aktiviert wird, kann das Konto keine Einladung von einem anderen Konto annehmen. Wenn ein Konto bereits eine Einladung angenommen hat, kann das Konto nicht durch das Security Hub CSPM-Administratorkonto für die Organisation aktiviert werden. Es kann auch keine Einladungen von anderen Konten empfangen.

Für den manuellen Einladungsprozess ist die Annahme einer Mitgliedschaftseinladung optional.

Mitgliedschaft durchAWS Organizations

Wenn Sie Security Hub CSPM mit integrierenAWS Organizations, kann das Verwaltungskonto der Organizations ein delegiertes Administratorkonto (DA) für Security Hub CSPM festlegen. Das Organisationsverwaltungskonto kann in Organizations nicht als DA festgelegt werden. Dies ist in Security Hub CSPM zwar zulässig, wir empfehlen jedoch, dass das Verwaltungskonto der Organizations nicht das DA sein sollte.

Wir empfehlen, dass Sie in allen Regionen dasselbe DA-Konto wählen. Wenn Sie die zentrale Konfiguration verwenden, richtet Security Hub CSPM in allen Regionen, in denen Sie Security Hub CSPM für Ihre Organisation konfigurieren, dasselbe DA-Konto ein.

Wir empfehlen außerdem, dass Sie für alle AWS Sicherheits- und Compliance-Dienste dasselbe DA-Konto wählen, damit Sie sicherheitsrelevante Probleme von einem zentralen Punkt aus verwalten können.

Mitgliedschaft auf Einladung

Bei Mitgliedskonten, die auf Einladung erstellt wurden, wird die Zuordnung zwischen Administrator und Mitgliedskonto nur in der Region erstellt, aus der die Einladung gesendet wurde. Das Administratorkonto muss Security Hub CSPM in jeder Region aktivieren, in der Sie es verwenden möchten. Das Administratorkonto lädt dann jedes Konto ein, ein Mitgliedskonto in dieser Region zu werden.

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten.

Koordination der Administratorkonten für alle Dienste

Security Hub CSPM fasst Ergebnisse verschiedener AWS Dienste wie Amazon GuardDuty, Amazon Inspector und Amazon Macie zusammen. Security Hub CSPM ermöglicht es Benutzern auch, von einem GuardDuty Ergebnis zu einer Untersuchung in Amazon Detective überzugehen.

Die Administrator-Mitglieds-Beziehungen, die Sie in diesen anderen Diensten einrichten, gelten jedoch nicht automatisch für Security Hub CSPM. Security Hub CSPM empfiehlt, dass Sie für all diese Dienste dasselbe Konto wie das Administratorkonto verwenden. Bei diesem Administratorkonto sollte es sich um ein Konto handeln, das für Sicherheitstools verantwortlich ist. Dasselbe Konto sollte auch das Aggregatorkonto für AWS Config sein.

Beispielsweise kann ein Benutzer des GuardDuty Administratorkontos A die Ergebnisse für die GuardDuty Mitgliedskonten B und C auf der GuardDuty Konsole sehen. Wenn Konto A dann Security Hub CSPM aktiviert, sehen Benutzer von Konto A nicht automatisch GuardDuty Ergebnisse für die Konten B und C in Security Hub CSPM. Für diese Konten ist auch eine Beziehung zwischen Security Hub CSPM-Administrator und Mitglied erforderlich.

Machen Sie dazu Konto A zum Security Hub CSPM-Administratorkonto und aktivieren Sie die Konten B und C als Security Hub CSPM-Mitgliedskonten.

Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations

Sie können AWS Security Hub CSPM in Security Hub CSPM integrieren und dann Security Hub CSPM für Konten in Ihrer Organisation verwalten. AWS Organizations

Um Security Hub CSPM zu integrierenAWS Organizations, erstellen Sie eine Organisation in. AWS Organizations Das Organisationsverwaltungskonto bestimmt ein Konto als delegierten Security Hub CSPM-Administrator für die Organisation. Der delegierte Administrator kann dann Security Hub CSPM für andere Konten in der Organisation aktivieren, diese Konten als Security Hub CSPM-Mitgliedskonten hinzufügen und zulässige Aktionen für die Mitgliedskonten ausführen. Der delegierte Security Hub CSPM-Administrator kann Security Hub CSPM für bis zu 10.000 Mitgliedskonten aktivieren und verwalten.

Der Umfang der Konfigurationsmöglichkeiten des delegierten Administrators hängt davon ab, ob Sie die zentrale Konfiguration verwenden. Wenn die zentrale Konfiguration aktiviert ist, müssen Sie Security Hub CSPM nicht in jedem Mitgliedskonto separat konfigurieren und. AWS-Region Der delegierte Administrator kann spezifische Security Hub CSPM-Einstellungen in bestimmten Mitgliedskonten und Organisationseinheiten (OUs) regionsübergreifend durchsetzen.

Das delegierte Security Hub-CSPM-Administratorkonto kann die folgenden Aktionen für Mitgliedskonten ausführen:

- Wenn Sie die zentrale Konfiguration verwenden, konfigurieren Sie Security Hub CSPM zentral für Mitgliedskonten und Organisationseinheiten, indem Sie Security Hub CSPM-Konfigurationsrichtlinien erstellen. Konfigurationsrichtlinien können verwendet werden, um Security Hub CSPM zu aktivieren und zu deaktivieren, Standards zu aktivieren und zu deaktivieren und Kontrollen zu aktivieren und zu deaktivieren.
- Behandeln Sie neue Konten automatisch als Security Hub CSPM-Mitgliedskonten, wenn sie der Organisation beitreten. Wenn Sie die zentrale Konfiguration verwenden, umfasst eine Konfigurationsrichtlinie, die einer Organisationseinheit zugeordnet ist, bestehende und neue Konten, die Teil der Organisationseinheit sind.
- Behandeln Sie bestehende Organisationskonten als Security Hub CSPM-Mitgliedskonten. Dies geschieht automatisch, wenn Sie die zentrale Konfiguration verwenden.
- Trennen Sie die Zuordnung von Mitgliedskonten, die zur Organisation gehören. Wenn Sie die zentrale Konfiguration verwenden, können Sie die Zuordnung eines Mitgliedskontos erst aufheben, nachdem Sie es als selbstverwaltet gekennzeichnet haben. Alternativ können Sie eine Konfigurationsrichtlinie, die Security Hub CSPM deaktiviert, bestimmten zentral verwalteten Mitgliedskonten zuordnen.

Wenn Sie sich nicht für die zentrale Konfiguration entscheiden, verwendet Ihr Unternehmen den Standardkonfigurationstyp, die als lokale Konfiguration bezeichnet wird. Bei der lokalen Konfiguration hat der delegierte Administrator eine eingeschränktere Möglichkeit, Einstellungen in Mitgliedskonten

durchzusetzen. Weitere Informationen finden Sie unter Grundlegendes zur lokalen Konfiguration in Security Hub CSPM.

Eine vollständige Liste der Aktionen, die der delegierte Administrator an Mitgliedskonten ausführen kann, finden Sie unter. Zulässige Aktionen von Administrator- und Mitgliedskonten in Security Hub CSPM

In den Themen dieses Abschnitts wird erklärt, wie Security Hub CSPM in Security Hub CSPM für Konten in einer Organisation integriert AWS Organizations und verwaltet wird. Wo relevant, werden in jedem Abschnitt die Verwaltungsvorteile und Unterschiede für Benutzer der zentralen Konfiguration aufgeführt.

Themen

- Integration von Security Hub CSPM mitAWS Organizations
- Automatisches Aktivieren von Security Hub CSPM in neuen Unternehmenskonten
- Manuelles Aktivieren von Security Hub CSPM in neuen Organisationskonten
- Trennung der Security Hub CSPM-Mitgliedskonten von Ihrer Organisation

Integration von Security Hub CSPM mitAWS Organizations

Um AWS Security Hub CSPM und zu integrierenAWS Organizations, erstellen Sie eine Organisation in Organizations und verwenden das Organisationsverwaltungskonto, um ein delegiertes Security Hub CSPM-Administratorkonto festzulegen. Dadurch wird Security Hub CSPM als vertrauenswürdiger Dienst in Organizations aktiviert. Es aktiviert auch Security Hub CSPM in der aktuellen Version AWS-Region für das delegierte Administratorkonto und ermöglicht es dem delegierten Administrator, Security Hub CSPM für Mitgliedskonten zu aktivieren, Daten in Mitgliedskonten anzuzeigen und andere zulässige Aktionen für Mitgliedskonten durchzuführen.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator auch Security Hub CSPM-Konfigurationsrichtlinien erstellen, die angeben, wie der Security Hub CSPM-Dienst, die Standards und Kontrollen in Organisationskonten konfiguriert werden sollen.

Erstellen einer Organisation

Eine Organisation ist eine Entität, die Sie erstellen, um Ihre Organisation zu konsolidieren, AWS-Konten sodass Sie sie als eine Einheit verwalten können.

Sie können eine Organisation entweder mithilfe der AWS Organizations Konsole oder mithilfe eines Befehls aus der AWS CLI oder einer der SDK-APIs erstellen. Ausführliche Anweisungen finden Sie im AWS OrganizationsBenutzerhandbuch unter Organisation erstellen.

Sie können AWS Organizations damit alle Konten in Ihrer Organisation zentral anzeigen und verwalten. Eine Organisation besteht aus einem Verwaltungskonto und gegebenenfalls Mitgliedskonten. Sie können die Konten in einer hierarchischen, baumähnlichen Struktur mit einem Stamm an der Spitze und Organisationseinheiten (OUs) unter dem Stamm organisieren. Jedes Konto kann sich direkt unter dem Stamm befinden oder in einer der Organisationseinheiten in der Hierarchie platziert werden. Eine OU ist ein Container für bestimmte Konten. Sie können beispielsweise eine Organisationseinheit für Finanzen erstellen, die alle Konten im Zusammenhang mit Finanzoperationen umfasst.

Empfehlungen für die Auswahl des delegierten Security Hub CSPM-Administrators

Wenn Sie über ein Administratorkonto aus dem manuellen Einladungsprozess verfügen und zur Kontoverwaltung mit wechseln, empfehlen wirAWS Organizations, dieses Konto als delegierten Security Hub CSPM-Administrator festzulegen.

Obwohl die Security Hub CSPM-APIs und die Konsole es dem Organisationsverwaltungskonto ermöglichen, der delegierte Security Hub CSPM-Administrator zu sein, empfehlen wir, zwei verschiedene Konten zu wählen. Dies liegt daran, dass Benutzer, die Zugriff auf das Organisationsverwaltungskonto haben, um die Abrechnung zu verwalten, sich wahrscheinlich von Benutzern unterscheiden, die für die Sicherheitsverwaltung Zugriff auf Security Hub CSPM benötigen.

Wir empfehlen, in allen Regionen denselben delegierten Administrator zu verwenden. Wenn Sie sich für die zentrale Konfiguration entscheiden, benennt Security Hub CSPM automatisch denselben delegierten Administrator in Ihrer Heimatregion und allen verknüpften Regionen.

Überprüfen Sie die Berechtigungen zur Konfiguration des delegierten Administrators

Um ein delegiertes Security Hub CSPM-Administratorkonto zuzuweisen und zu entfernen, muss das Organisationsverwaltungskonto über Berechtigungen für die `DisableOrganizationAdminAccount` Aktionen `EnableOrganizationAdminAccount` und in Security Hub CSPM verfügen. Das Verwaltungskonto für Organizations muss auch über Administratorberechtigungen für Organizations verfügen.

Um alle erforderlichen Berechtigungen zu gewähren, fügen Sie dem IAM-Prinzipal für das Organisationsverwaltungskonto die folgenden von Security Hub verwalteten CSPM-Richtlinien hinzu:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Benennen des delegierten Administrators

Um das delegierte Security Hub CSPM-Administratorkonto festzulegen, können Sie die Security Hub CSPM-Konsole, die Security Hub CSPM-API oder verwenden. AWS CLI Security Hub CSPM legt den delegierten Administrator AWS-Region nur in der aktuellen Region fest, und Sie müssen die Aktion in anderen Regionen wiederholen. Wenn Sie die zentrale Konfiguration verwenden, richtet Security Hub CSPM automatisch denselben delegierten Administrator in der Heimatregion und den verknüpften Regionen ein.

Das Organisationsverwaltungskonto muss Security Hub CSPM nicht aktivieren, um das delegierte Security Hub CSPM-Administratorkonto zu bestimmen.

Wir empfehlen, dass das Organisationsverwaltungskonto nicht das delegierte Security Hub CSPM-Administratorkonto ist. Wenn Sie jedoch das Organisationsverwaltungskonto als delegierten Security Hub CSPM-Administrator wählen, muss Security Hub CSPM für das Verwaltungskonto aktiviert sein. Wenn Security Hub CSPM für das Verwaltungskonto nicht aktiviert ist, müssen Sie Security Hub CSPM manuell dafür aktivieren. Security Hub CSPM kann nicht automatisch für das Organisationsverwaltungskonto aktiviert werden.

Sie müssen den delegierten Security Hub CSPM-Administrator mit einer der folgenden Methoden benennen. Die Benennung des delegierten Security Hub CSPM-Administrators mit Organisations-APIs spiegelt sich nicht in Security Hub CSPM wider.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Benennung des delegierten Security Hub CSPM-Administratorkontos.

Security Hub CSPM console

Um den delegierten Administrator beim Onboarding zu bestimmen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie Gehe zu Security Hub CSPM. Sie werden aufgefordert, sich mit dem Organisationsverwaltungskonto anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator benennen im Abschnitt Delegiertes Administratorkonto das delegierte Administratorkonto an. Wir empfehlen, denselben

delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben.

4. Wählen Sie Als delegierten Administrator festlegen aus. Sie werden aufgefordert, sich mit dem delegierten Administratorkonto anzumelden (falls Sie dies noch nicht getan haben), um das Onboarding mit der zentralen Konfiguration fortzusetzen. Wenn Sie die zentrale Konfiguration nicht starten möchten, wählen Sie Abbrechen. Ihr delegierter Administrator ist eingerichtet, aber Sie verwenden die zentrale Konfiguration noch nicht.

Um den delegierten Administrator aus dem Einstellungen angezeigten

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Einstellungen aus. Wählen Sie dann Allgemein.
3. Wenn derzeit ein Security Hub CSPM-Administratorkonto zugewiesen ist, müssen Sie das aktuelle Konto entfernen, bevor Sie ein neues Konto einrichten können.

   Um das aktuelle Konto zu entfernen, wählen Sie unter Delegierter Administrator die Option Entfernen aus.
4. Geben Sie die Konto-ID des Kontos ein, das Sie als Security Hub CSPM-Administratorkonto festlegen möchten.

   Sie müssen in allen Regionen dasselbe Security Hub CSPM-Administratorkonto angeben. Wenn Sie ein Konto angeben, das sich von dem in anderen Regionen angegebenen Konto unterscheidet, gibt die Konsole einen Fehler zurück.
5. Wählen Sie Delegieren.

Security Hub CSPM API,AWS CLI

Verwenden Sie vom Organisationsverwaltungskonto aus den EnableOrganizationAdminAccountBetrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den enable-organization-admin-accountBefehl aus. Geben Sie die AWS-Konto ID des delegierten Security Hub CSPM-Administrators an.

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator benannt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Den delegierten Administrator entfernen oder ändern

Nur das Organisationsverwaltungskonto kann das delegierte Security Hub CSPM-Administratorkonto entfernen.

Um den delegierten Security Hub CSPM-Administrator zu ändern, müssen Sie zuerst das aktuelle delegierte Administratorkonto entfernen und dann ein neues festlegen.

> **Warning**
>
> Wenn Sie die zentrale Konfiguration verwenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-APIs nicht verwenden, um das delegierte Administratorkonto zu ändern oder zu entfernen. Wenn das Organisationsverwaltungskonto die AWS Organizations Konsole oder AWS Organizations APIs verwendet, um den delegierten Security Hub CSPM-Administrator zu ändern oder zu entfernen, stoppt Security Hub CSPM automatisch die zentrale Konfiguration und löscht Ihre Konfigurationsrichtlinien und Richtlinienzuordnungen. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Wenn Sie die Security Hub CSPM-Konsole verwenden, um den delegierten Administrator in einer Region zu entfernen, wird er automatisch in allen Regionen entfernt.

Die Security Hub CSPM API entfernt nur das delegierte Security Hub CSPM-Administratorkonto aus der Region, in der der API-Aufruf oder -Befehl ausgeführt wird. Sie müssen die Aktion in anderen Regionen wiederholen.

Wenn Sie das delegierte Security Hub CSPM-Administratorkonto mit der Organizations-API entfernen, wird es automatisch in allen Regionen entfernt.

Den delegierten Administrator entfernen (Organizations API,AWS CLI)

Sie können Organizations verwenden, um den delegierten Security Hub CSPM-Administrator in allen Regionen zu entfernen.

Wenn Sie die zentrale Konfiguration zur Verwaltung von Konten verwenden, führt das Entfernen des delegierten Administratorkontos zum Löschen Ihrer Konfigurationsrichtlinien und

Richtlinienverknüpfungen. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde. Diese Konten können jedoch nicht mehr mit dem entfernten delegierten Administratorkonto verwaltet werden. Sie werden zu selbstverwalteten Konten, die in jeder Region separat konfiguriert werden müssen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen, um das delegierte Security Hub CSPM-Administratorkonto mit zu entfernen. AWS Organizations

Organizations API,AWS CLI

So entfernen Sie den delegierten Security Hub CSPM-Administrator

Verwenden Sie vom Organisationsverwaltungskonto aus den DeregisterDelegatedAdministratorBetrieb der Organisations-API. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl deregister-delegated-administrator aus. Geben Sie die Konto-ID des delegierten Administrators und den Dienstprinzipal für Security Hub CSPM an, nämlich. `securityhub.amazonaws.com`

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator entfernt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Den delegierten Administrator entfernen (Security Hub CSPM-Konsole)

Sie können die Security Hub CSPM-Konsole verwenden, um den delegierten Security Hub CSPM-Administrator in allen Regionen zu entfernen.

Wenn das delegierte Security Hub CSPM-Administratorkonto entfernt wird, werden die Mitgliedskonten vom entfernten delegierten Security Hub CSPM-Administratorkonto getrennt.

Security Hub CSPM ist weiterhin in den Mitgliedskonten aktiviert. Sie werden zu eigenständigen Konten, bis ein neuer Security Hub CSPM-Administrator sie als Mitgliedskonten aktiviert.

Wenn das Organisationsverwaltungskonto kein aktiviertes Konto in Security Hub CSPM ist, verwenden Sie die Option auf der Seite Willkommen bei Security Hub CSPM.

Um das delegierte Security Hub CSPM-Administratorkonto aus dem Willkommen bei Security Hub CSPM angezeigten

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie Gehe zu Security Hub.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Wenn das Organisationsverwaltungskonto ein aktiviertes Konto in Security Hub ist, verwenden Sie die Option auf der Registerkarte Allgemein der Seite Einstellungen.

Um das delegierte Security Hub CSPM-Administratorkonto aus dem Einstellungen angezeigten

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Einstellungen aus. Wählen Sie dann Allgemein.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Den delegierten Administrator entfernen (Security Hub CSPM API,AWS CLI)

Sie können die Security Hub CSPM-API oder die Security Hub CSPM-Operationen verwenden, AWS CLI um den delegierten Security Hub CSPM-Administrator zu entfernen. Wenn Sie den delegierten Administrator mit einer dieser Methoden entfernen, wird er nur in der Region entfernt, in der der API-Aufruf oder -Befehl ausgeführt wurde. Security Hub CSPM aktualisiert keine anderen Regionen und entfernt auch nicht das delegierte Administratorkonto in. AWS Organizations

Wählen Sie Ihre bevorzugte Methode und gehen Sie wie folgt vor, um das delegierte Security Hub CSPM-Administratorkonto bei Security Hub CSPM zu entfernen.

Security Hub CSPM API,AWS CLI

So entfernen Sie den delegierten Security Hub CSPM-Administrator

Verwenden Sie vom Organisationsverwaltungskonto aus den DisableOrganizationAdminAccountBetrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den disable-organization-admin-accountBefehl aus. Geben Sie die Konto-ID des delegierten Security Hub CSPM-Administrators an.

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator entfernt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Deaktivieren der Security Hub CSPM-Integration mitAWS Organizations

Nachdem eine AWS Organizations Organisation in AWS Security Hub CSPM integriert wurde, kann das Verwaltungskonto der Organizations die Integration anschließend deaktivieren. Als Benutzer des Organisationsverwaltungskontos können Sie dies tun, indem Sie den vertrauenswürdigen Zugriff für Security Hub CSPM in deaktivieren. AWS Organizations

Wenn Sie den vertrauenswürdigen Zugriff für Security Hub CSPM deaktivieren, passiert Folgendes:

- Security Hub CSPM verliert seinen Status als vertrauenswürdiger Dienst in. AWS Organizations
- Das delegierte Security Hub CSPM-Administratorkonto verliert den Zugriff auf Security Hub CSPM-Einstellungen, Daten und Ressourcen für alle Security Hub CSPM-Mitgliedskonten insgesamt. AWS-Regionen
- Wenn Sie die zentrale Konfiguration verwendet haben, verwendet Security Hub CSPM sie automatisch nicht mehr für Ihr Unternehmen. Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen werden gelöscht. Konten behalten die Konfigurationen bei, die sie hatten, bevor Sie den vertrauenswürdigen Zugriff deaktiviert haben.
- Alle Security Hub CSPM-Mitgliedskonten werden zu eigenständigen Konten und behalten ihre aktuellen Einstellungen bei. Wenn Security Hub CSPM für ein Mitgliedskonto in einer oder mehreren Regionen aktiviert wurde, ist Security Hub CSPM weiterhin für das Konto in diesen Regionen aktiviert. Die aktivierten Standards und Kontrollen bleiben ebenfalls unverändert. Sie können diese Einstellungen für jedes Konto und jede Region separat ändern. Das Konto ist jedoch in keiner Region mehr mit einem delegierten Administrator verknüpft.

Weitere Informationen zu den Ergebnissen der Deaktivierung des Zugriffs auf vertrauenswürdige Dienste finden Sie AWS-Services im AWS OrganizationsBenutzerhandbuch unter AWS Organizations Zusammen mit anderen Benutzern verwenden.

Um den vertrauenswürdigen Zugriff zu deaktivieren, können Sie die AWS Organizations Konsole, die Organisations-API oder die verwendenAWS CLI. Nur ein Benutzer des

Organisationsverwaltungskontos kann den vertrauenswürdigen Dienstzugriff für Security Hub CSPM deaktivieren. Einzelheiten zu den Berechtigungen, die Sie benötigen, finden Sie im AWS OrganizationsBenutzerhandbuch unter Erforderliche Berechtigungen zur Deaktivierung des vertrauenswürdigen Zugriffs.

Bevor Sie den vertrauenswürdigen Zugriff deaktivieren, empfehlen wir, mit dem delegierten Administrator Ihrer Organisation zusammenzuarbeiten, um Security Hub CSPM in Mitgliedskonten zu deaktivieren und die Security Hub CSPM-Ressourcen in diesen Konten zu bereinigen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den vertrauenswürdigen Zugriff für Security Hub CSPM zu deaktivieren.

Organizations console

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

1. Melden Sie sich AWS-Managementkonsole mit den Anmeldeinformationen des AWS Organizations Verwaltungskontos an.
2. Öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
3. Wählen Sie im Navigationsbereich Services.
4. Wählen Sie unter Integrierte Dienste die Option AWSSecurity Hub CSPM aus.
5. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
6. Bestätigen Sie, dass Sie den vertrauenswürdigen Zugriff deaktivieren möchten.

Organizations API

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

Rufen Sie den DisableAWSServiceAccessBetrieb der API auf. AWS Organizations Geben Sie für den `ServicePrincipal` Parameter den Security Hub CSPM-Dienstprinzipal () `securityhub.amazonaws.com` an.

AWS CLI

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

Führen Sie den Befehl disable-aws-service-access der API aus. AWS Organizations Geben Sie für den `service-principal` Parameter den Security Hub CSPM-Dienstprinzipal () `securityhub.amazonaws.com` an.

Beispiel:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Automatisches Aktivieren von Security Hub CSPM in neuen Unternehmenskonten

Wenn neue Konten Ihrer Organisation beitreten, werden sie der Liste auf der Kontoseite der AWS Security Hub CSPM-Konsole hinzugefügt. Für Organisationskonten lautet Typ auf Nach Organisation. Standardmäßig werden neue Konten nicht zu Security Hub CSPM-Mitgliedern, wenn sie der Organisation beitreten. Ihr Status ist Kein Mitglied. Das delegierte Administratorkonto kann automatisch neue Konten als Mitglieder hinzufügen und Security Hub CSPM in diesen Konten aktivieren, wenn sie der Organisation beitreten.

> **Note**
>
> Obwohl viele Regionen standardmäßig für Sie aktiv AWS-Regionen sindAWS-Konto, müssen Sie bestimmte Regionen manuell aktivieren. Diese Regionen werden in diesem Dokument als Opt-in-Regionen bezeichnet. Um Security Hub CSPM automatisch in einem neuen Konto in einer Opt-in-Region zu aktivieren, muss diese Region zuerst für das Konto aktiviert sein. Nur der Kontoinhaber kann die Opt-in-Region aktivieren. Weitere Informationen zu Opt-in-Regionen finden Sie unter Geben Sie an, welche Regionen AWS-Regionen Ihr Konto verwenden kann.

Dieser Vorgang unterscheidet sich je nachdem, ob Sie die zentrale Konfiguration (empfohlen) oder die lokale Konfiguration verwenden.

Automatische Aktivierung neuer Organisationskonten (zentrale Konfiguration)

Wenn Sie die zentrale Konfiguration verwenden, können Sie Security Hub CSPM automatisch in neuen und bestehenden Organisationskonten aktivieren, indem Sie eine Konfigurationsrichtlinie erstellen, in der Security Hub CSPM aktiviert ist. Anschließend können Sie die Richtlinie dem Organisationsstamm oder bestimmten Organisationseinheiten (OUs) zuordnen.

Wenn Sie eine Konfigurationsrichtlinie, in der Security Hub CSPM aktiviert ist, einer bestimmten OU zuordnen, wird Security Hub CSPM automatisch in allen Konten (vorhandenen und neuen) aktiviert, die zu dieser OU gehören. Neue Konten, die nicht zur Organisationseinheit gehören, werden

selbst verwaltet und Security Hub CSPM ist nicht automatisch aktiviert. Wenn Sie dem Root eine Konfigurationsrichtlinie zuordnen, in der Security Hub CSPM aktiviert ist, wird Security Hub CSPM automatisch in allen Konten (vorhandenen und neuen) aktiviert, die der Organisation beitreten. Ausnahmen sind, wenn ein Konto aufgrund von Anwendung oder Vererbung eine andere Richtlinie verwendet oder wenn es sich um ein selbstverwaltetes Konto handelt.

In Ihrer Konfigurationsrichtlinie können Sie auch definieren, welche Sicherheitsstandards und Kontrollen in der Organisationseinheit aktiviert werden sollen. Um Kontrollergebnisse für aktivierte Standards zu generieren, müssen die Konten in der Organisationseinheit AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter Aktivieren und Konfigurieren AWS Config.

Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unterKonfigurationsrichtlinien erstellen und zuordnen.

Automatisches Aktivieren neuer Organisationskonten (lokale Konfiguration)

Wenn Sie die lokale Konfiguration verwenden und die automatische Aktivierung von Standardstandards aktivieren, fügt Security Hub CSPM neue Organisationskonten als Mitglieder hinzu und aktiviert Security Hub CSPM in diesen Konten in der aktuellen Region. Andere Regionen sind nicht betroffen. Darüber hinaus aktiviert die Aktivierung der automatischen Aktivierung Security Hub CSPM nicht in bestehenden Organisationskonten, es sei denn, sie wurden bereits als Mitgliedskonten hinzugefügt.

Nach der Aktivierung der automatischen Aktivierung werden die Standardsicherheitsstandards für neue Mitgliedskonten in der aktuellen Region aktiviert, wenn sie der Organisation beitreten. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Sie können die Standardstandards nicht ändern. Wenn Sie in Ihrer Organisation andere Standards oder Standards für ausgewählte Konten und Organisationseinheiten aktivieren möchten, empfehlen wir die zentrale Konfiguration.

Um Kontrollergebnisse für die Standardstandards (und andere aktivierte Standards) zu generieren, müssen die Konten in Ihrer Organisation AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter Aktivieren und Konfigurieren AWS Config.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub CSPM automatisch in neuen Unternehmenskonten zu aktivieren. Diese Anweisungen gelten nur, wenn Sie die lokale Konfiguration verwenden.

Security Hub CSPM console

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Sign verwendet die Anmeldeinformationen des delegierten Administratorkontos.
2. Wählen Sie im Security Hub CSPM-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Aktivieren Sie im Abschnitt Konten die Option Konten. Auto-enable

Security Hub CSPM API

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

Rufen Sie die `UpdateOrganizationConfiguration`API vom delegierten Administratorkonto aus auf. Setzen Sie das `AutoEnable` Feld auf, `true` um Security Hub CSPM automatisch in neuen Organisationskonten zu aktivieren.

AWS CLI

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

Führen Sie den `update-organization-configuration`Befehl über das delegierte Administratorkonto aus. Fügen Sie den `auto-enable` Parameter hinzu, um Security Hub CSPM automatisch in neuen Organisationskonten zu aktivieren.

```
aws securityhub update-organization-configuration --auto-enable
```

Manuelles Aktivieren von Security Hub CSPM in neuen Organisationskonten

Wenn Sie Security Hub CSPM nicht automatisch in neuen Organisationskonten aktivieren, wenn diese der Organisation beitreten, können Sie diese Konten als Mitglieder hinzufügen und Security Hub CSPM in ihnen manuell aktivieren, nachdem sie der Organisation beigetreten sind. Sie müssen Security Hub CSPM auch manuell aktivieren, da Sie zuvor AWS-Konten die Verbindung zu einer Organisation getrennt haben.

> **Note**
>
> Dieser Abschnitt gilt nicht für Sie, wenn Sie die zentrale Konfiguration verwenden. Wenn Sie die zentrale Konfiguration verwenden, können Sie Konfigurationsrichtlinien erstellen, die Security Hub CSPM in bestimmten Mitgliedskonten und Organisationseinheiten (OUs) aktivieren. Sie können auch spezifische Standards und Kontrollen für diese Konten und Organisationseinheiten aktivieren.

Sie können Security Hub CSPM nicht in einem Konto aktivieren, wenn es sich bereits um ein Mitgliedskonto in einer anderen Organisation handelt.

Sie können Security Hub CSPM auch nicht in einem Konto aktivieren, das derzeit gesperrt ist. Wenn Sie versuchen, den Dienst in einem gesperrten Konto zu aktivieren, ändert sich der Kontostatus in Konto gesperrt.

- Wenn Security Hub CSPM für das Konto nicht aktiviert ist, ist Security Hub CSPM in diesem Konto aktiviert. Der Standard AWS Foundational Security Best Practices (FSBP) und der CIS AWS Foundations Benchmark v1.2.0 sind ebenfalls im Konto aktiviert, sofern Sie die Standardsicherheitsstandards nicht deaktivieren.

  Eine Ausnahme bildet das Verwaltungskonto für Organizations. Security Hub CSPM kann nicht automatisch im Verwaltungskonto der Organizations aktiviert werden. Sie müssen Security Hub CSPM manuell im Verwaltungskonto der Organizations aktivieren, bevor Sie es als Mitgliedskonto hinzufügen können.
- Wenn Security Hub CSPM für das Konto bereits aktiviert ist, nimmt Security Hub CSPM keine weiteren Änderungen am Konto vor. Es aktiviert nur die Mitgliedschaft.

Damit Security Hub CSPM Kontrollergebnisse generieren kann, müssen Mitgliedskonten AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur Konfiguration von SSH finden Sie unter Aktivieren und Konfigurieren von AWS Config.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Organisationskonto als Security Hub CSPM-Mitgliedskonto zu aktivieren.

Security Hub CSPM console

Um Unternehmenskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.
2. Wählen Sie im Security Hub CSPM-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie in der Kontenliste jedes Unternehmenskonto aus, das Sie aktivieren möchten.
4. Wählen Sie Aktionen und dann Mitglied hinzufügen aus.

Security Hub CSPM API

Um Unternehmenskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

Rufen Sie die `CreateMembers`API vom delegierten Administratorkonto aus auf. Geben Sie für jedes zu aktivierende Konto die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess müssen `CreateMembers` Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

AWS CLI

Um Unternehmenskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

Führen Sie den `create-members`Befehl über das delegierte Administratorkonto aus. Geben Sie für jedes zu aktivierende Konto die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess `create-members` müssen Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Trennung der Security Hub CSPM-Mitgliedskonten von Ihrer Organisation

Wenn Sie keine Ergebnisse von einem AWS Security Hub CSPM-Mitgliedskonto mehr erhalten und einsehen möchten, können Sie das Mitgliedskonto von Ihrer Organisation trennen.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, funktioniert die Trennung anders. Sie können eine Konfigurationsrichtlinie erstellen, die Security Hub CSPM in einem oder mehreren zentral verwalteten Mitgliedskonten deaktiviert. Danach sind diese Konten immer noch Teil der Organisation, generieren aber keine CSPM-Ergebnisse von Security Hub. Wenn Sie die zentrale Konfiguration verwenden, aber auch über manuell eingeladene Mitgliedskonten verfügen, können Sie die Zuordnung zu einem oder mehreren manuell eingeladenen Konten aufheben.

Mitgliedskonten, die über verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur das Administratorkonto kann die Zuordnung eines Mitgliedskontos aufheben.

Durch die Trennung eines Mitgliedskontos wird das Konto nicht geschlossen. Stattdessen wird das Mitgliedskonto aus der Organisation entfernt. Das getrennte Mitgliedskonto wird zu einem eigenständigen KontoAWS-Konto, das nicht mehr von der Security Hub CSPM-Integration mit verwaltet wird. AWS Organizations

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Mitgliedskonto von der Organisation zu trennen.

Security Hub CSPM console

Um ein Mitgliedskonto von der Organisation zu trennen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten. Wenn Sie die zentrale Konfiguration verwenden, können Sie auf der Registerkarte ein

manuell eingerichtetes Konto auswählen, dessen Verbindung aufgehoben werden soll. `Invitation accounts` Diese Registerkarte ist nur sichtbar, wenn Sie die zentrale Konfiguration verwenden.

4. Wählen Sie Aktionen und anschließend Konto trennen aus.

Security Hub CSPM API

Um ein Mitgliedskonto von der Organisation zu trennen

Rufen Sie die `DisassociateMembers`API vom delegierten Administratorkonto aus auf. Sie müssen die AWS-Konto IDs für die Mitgliedskonten angeben, um die Zuordnung aufzuheben. Rufen Sie die API auf, um eine Liste der Mitgliedskonten anzuzeigen. `ListMembers`

AWS CLI

Um ein Mitgliedskonto von der Organisation zu trennen

Führen Sie den `disassociate-members` Befehl > vom delegierten Administratorkonto aus. Sie müssen die AWS-Konto IDs für die Mitgliedskonten angeben, um die Zuordnung aufzuheben. Um eine Liste der Mitgliedskonten anzuzeigen, führen Sie den `list-members` Befehl > aus.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Sie können auch die AWS Organizations Konsole oder AWS SDKs verwendenAWS CLI, um die Zuordnung eines Mitgliedskontos zu Ihrer Organisation aufzuheben. Weitere Informationen finden Sie im AWS OrganizationsBenutzerhandbuch unter Entfernen eines Mitgliedskontos aus Ihrer Organisation.

Konten auf Einladung in Security Hub CSPM verwalten

Sie können mehrere AWS Security Hub CSPM-Konten auf zwei Arten zentral verwalten: durch die Integration von Security Hub CSPM in AWS Organizations oder durch manuelles Senden und Akzeptieren von Mitgliedschaftseinladungen. Sie müssen den manuellen Prozess verwenden, wenn Sie ein eigenständiges Konto haben oder nicht integrieren möchten. AWS Organizations Bei der

manuellen Kontoverwaltung lädt der Security Hub CSPM-Administrator Konten ein, Mitglieder zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitglied die Einladung annimmt. Ein Security Hub CSPM-Administratorkonto kann Security Hub CSPM für bis zu 1.000 Mitgliedskonten verwalten, die auf Einladung basieren.

> **Note**
>
> Wenn Sie in Security Hub CSPM eine Organisation erstellen, die auf Einladung basiert, können Sie anschließend auf die Verwendung von CSPM umsteigen. AWS Organizations Wenn Sie mehr als ein Mitgliedskonto haben, empfehlen wir, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Cross-Region Die Zusammenfassung von Ergebnissen und anderen Daten ist für Konten verfügbar, die Sie über den manuellen Einladungsprozess einladen. Der Administrator muss jedoch das Mitgliedskonto aus der Aggregationsregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss für das Mitgliedskonto Security Hub CSPM in der Aggregationsregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann.

Konfigurationsrichtlinien werden für manuell eingeladene Mitgliedskonten nicht unterstützt. Stattdessen müssen Sie die Security Hub CSPM-Einstellungen in jedem Mitgliedskonto und AWS-Region bei Verwendung des manuellen Einladungsprozesses separat konfigurieren.

Sie müssen den manuellen Einladungsprozess auch für Konten verwenden, die nicht zu Ihrer Organisation gehören. Beispielsweise könnten Sie in Ihrer Organisation kein Testkonto einrichten. Oder vielleicht möchten Sie Konten mehrerer Organisationen unter einem einzigen Security Hub CSPM-Administratorkonto konsolidieren. Das Security Hub CSPM-Administratorkonto muss Einladungen an Konten senden, die anderen Organisationen gehören.

Auf der Konfigurationsseite der Security Hub CSPM-Konsole werden Konten, die auf Einladung hinzugefügt wurden, auf der Registerkarte Einladungskonten aufgeführt. Wenn Sie die zentrale Konfiguration verwenden, aber auch Konten außerhalb Ihrer Organisation einladen, können Sie sich auf dieser Registerkarte die Ergebnisse von Konten ansehen, die auf Einladungen basieren. Der Security Hub CSPM-Administrator kann jedoch mithilfe von Konfigurationsrichtlinien keine Konten, die auf Einladungen basieren, regionsübergreifend konfigurieren.

In den Themen in diesem Abschnitt wird erklärt, wie Mitgliedskonten mithilfe von Einladungen verwaltet werden.

Themen

- Mitgliedskonten in Security Hub CSPM hinzufügen und einladen
- Auf eine Einladung antworten, ein Security Hub CSPM-Mitgliedskonto zu werden
- Aufheben der Zuordnung von Mitgliedskonten in Security Hub CSPM
- Löschen von Mitgliedskonten in Security Hub CSPM
- Trennung von einem Security Hub CSPM-Administratorkonto
- Umstellung auf Organizations zur Verwaltung von Konten in Security Hub CSPM

Mitgliedskonten in Security Hub CSPM hinzufügen und einladen

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Ihr Konto wird zum AWS Security Hub CSPM-Administrator für Konten, die Ihre Einladung annehmen, ein Security Hub CSPM-Mitgliedskonto zu werden.

Wenn Sie eine Einladung von einem anderen Konto annehmen, wird Ihr Konto zu einem Mitgliedskonto und dieses Konto wird zu Ihrem Administrator.

Wenn es sich bei Ihrem Konto um ein Administratorkonto handelt, können Sie eine Einladung, ein Mitgliedskonto zu werden, nicht annehmen.

Das Hinzufügen eines Mitgliedskontos besteht aus den folgenden Schritten:

1. Das Administratorkonto fügt das Mitgliedskonto zu seiner Liste der Mitgliedskonten hinzu.
2. Das Administratorkonto sendet eine Einladung an das Mitgliedskonto.
3. Das Mitgliedskonto akzeptiert die Einladung.

Mitgliedskonten hinzufügen

Von der Security Hub CSPM-Konsole aus können Sie Konten zu Ihrer Liste der Mitgliedskonten hinzufügen. In der Security Hub CSPM-Konsole können Sie Konten einzeln auswählen oder eine `.csv` Datei hochladen, die die Kontoinformationen enthält.

Für jedes Konto müssen Sie die Konto-ID und eine E-Mail-Adresse angeben. Die E-Mail-Adresse sollte die E-Mail-Adresse sein, an die Sie sich bei Sicherheitsproblemen im Konto wenden können. Sie wird nicht zur Verifizierung des Kontos verwendet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Hinzufügen von Mitgliedskonten.

Security Hub CSPM console

Um Konten zu deiner Liste von Mitgliedskonten hinzuzufügen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im linken Bereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Option Konten und dann Konten hinzufügen aus. Sie können dann entweder einzelne Konten hinzufügen oder eine `.csv` Datei hochladen, die die Liste der Konten enthält.
4. Gehen Sie wie folgt vor, um die Konten auszuwählen:

   - Um die Konten einzeln hinzuzufügen, geben Sie unter Konten eingeben die Konto-ID und die E-Mail-Adresse des hinzuzufügenden Kontos ein, und wählen Sie dann Hinzufügen aus.

     Wiederholen Sie diesen Vorgang für jedes Konto.
   - Um eine Datei mit kommagetrennten Werten (.csv) zum Hinzufügen mehrerer Konten zu verwenden, erstellen Sie zunächst die Datei. Die Datei muss die Konto-ID und die E-Mail-Adresse für jedes hinzuzufügende Konto enthalten.

     In Ihrer `.csv` Liste muss eines pro Zeile erscheinen. Die erste Zeile der `.csv` Datei muss den Header enthalten. In der Kopfzeile befindet sich die erste Spalte **`Account ID`** und die zweite Spalte ist**`Email`**.

Jede weitere Zeile muss eine gültige Konto-ID und eine gültige E-Mail-Adresse für das Konto enthalten, das Sie hinzufügen möchten.

Hier ist ein Beispiel für eine `.csv` Datei, wenn sie in einem Texteditor angezeigt wird.

```
Account ID,Email
111111111111,user@example.com
```

In einem Tabellenkalkulationsprogramm werden die Felder in separaten Spalten angezeigt. Das zugrunde liegende Format ist immer noch durch Kommas getrennt. Sie müssen die Konto-IDs als Zahlen ohne Dezimalzahlen formatieren. Beispielsweise kann die Konto-ID 444455556666 nicht als 444455556666.0 formatiert werden. Stellen Sie außerdem sicher, dass bei der Zahlenformatierung keine führenden Nullen aus der Konto-ID entfernt werden.

Um die Datei auszuwählen, wählen Sie auf der Konsole die Option Liste hochladen (.csv). Wählen Sie dann „Durchsuchen“.

Nachdem Sie die Datei ausgewählt haben, wählen Sie Konten hinzufügen.

5. Wenn Sie mit dem Hinzufügen von Konten fertig sind, wählen Sie unter Hinzuzufügende Konten die Option Weiter aus.

Security Hub CSPM API

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Rufen Sie die `CreateMembers`API vom Administratorkonto aus auf. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Führen Sie den `create-members`Befehl vom Administratorkonto aus. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Mitgliedskonten einladen

Nachdem Sie die Mitgliedskonten hinzugefügt haben, senden Sie eine Einladung an das Mitgliedskonto. Sie können eine Einladung auch erneut an ein Konto senden, das Sie vom Administrator getrennt haben.

Security Hub CSPM console

Um Konten potenzieller Mitglieder einzuladen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie für das einzuladende Konto Invite (Einladen) in der Spalte Status aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Einladen.

> **Note**
>
> Um Einladungen an getrennte Konten erneut zu senden, wählen Sie auf der Seite Konten jedes getrennte Konto aus. Wählen Sie unter Aktionen die Option Einladung erneut senden aus.

Security Hub CSPM API

Um Konten potenzieller Mitglieder einzuladen

Rufen Sie die `InviteMembers`API vom Administratorkonto aus auf. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten potenzieller Mitglieder einzuladen

Führen Sie den `invite-members`Befehl vom Administratorkonto aus. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Beispiel

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Auf eine Einladung antworten, ein Security Hub CSPM-Mitgliedskonto zu werden

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Sie können eine Einladung als AWS Security Hub CSPM-Mitgliedskonto annehmen oder ablehnen.

Wenn Sie eine Einladung annehmen, wird Ihr Konto zu einem Security Hub CSPM-Mitgliedskonto. Das Konto, das die Einladung gesendet hat, wird zu Ihrem Security Hub CSPM-Administratorkonto. Der Benutzer des Administratorkontos kann die Ergebnisse für Ihr Mitgliedskonto in Security Hub CSPM einsehen.

Wenn Sie die Einladung ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als Kündigt markiert.

Sie können nur eine Einladung annehmen, ein Mitgliedskonto zu werden.

Bevor Sie eine Einladung annehmen oder ablehnen können, müssen Sie Security Hub CSPM aktivieren.

Denken Sie daran, dass alle Security Hub CSPM-Konten AWS Config aktiviert und konfiguriert sein müssen, um alle Ressourcen aufzuzeichnen. Einzelheiten zu den Anforderungen für finden Sie AWS Config unter Aktivierung und Konfiguration. AWS Config

Eine Einladung annehmen

Sie können vom Administratorkonto aus eine Einladung senden, ein Security Hub CSPM-Mitgliedskonto zu werden. Sie können die Einladung dann annehmen, nachdem Sie sich mit dem Mitgliedskonto angemeldet haben.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto anzunehmen.

Security Hub CSPM console

Um eine Einladung zur Mitgliedschaft anzunehmen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Aktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Einladung annehmen aus.

Security Hub CSPM API

Um eine Einladung zur Mitgliedschaft anzunehmen

Rufen Sie die `AcceptAdministratorInvitation`API auf. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Verwenden Sie den `ListInvitations`Vorgang, um Details zur Einladung abzurufen.

AWS CLI

Um eine Einladung zur Mitgliedschaft anzunehmen

Führen Sie den Befehl `accept-administrator-invitation` aus. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Führen Sie den `list-invitations`Befehl aus, um Details zur Einladung abzurufen.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Beispiel

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Die Security Hub CSPM-Konsole wird weiterhin verwendet. `AcceptInvitation` Sie wird irgendwann auf Verwendung umgestellt. `AcceptAdministratorInvitation` Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion regeln, müssen weiterhin verwendet `AcceptInvitation` werden. Sie sollten Ihre Richtlinien auch ergänzen`AcceptAdministratorInvitation`, um sicherzustellen, dass nach Beginn der Nutzung `AcceptAdministratorInvitation` der Konsole die richtigen Berechtigungen vorhanden sind.

Eine Einladung ablehnen

Sie können eine Einladung, ein Security Hub CSPM-Mitgliedskonto zu werden, ablehnen. Wenn Sie eine Einladung in der Security Hub CSPM-Konsole ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als Signiert markiert. Der Status Kündigt wird nur angezeigt, wenn Sie sich mit dem Administratorkonto bei der Security Hub CSPM-Konsole anmelden. Die Einladung bleibt jedoch unverändert in der Konsole für das Mitgliedskonto, bis Sie sich beim Administratorkonto anmelden und die Einladung löschen.

Um eine Einladung abzulehnen, müssen Sie sich bei dem Mitgliedskonto anmelden, das die Einladung erhalten hat.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto abzulehnen.

Security Hub CSPM console

Um eine Einladung zur Mitgliedschaft abzulehnen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie im Abschnitt Administratorkonto die Option Einladung ablehnen aus.

Security Hub CSPM API

Um eine Einladung zur Mitgliedschaft abzulehnen

Rufen Sie die `DeclineInvitations`API auf. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Verwenden Sie den `ListInvitations`Vorgang, um Informationen zu Ihren Einladungen anzuzeigen.

AWS CLI

Um eine Einladung zur Mitgliedschaft abzulehnen

Führen Sie den Befehl `decline-invitations` aus. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Führen Sie den `list-invitations`Befehl aus, um Informationen zu Ihren Einladungen anzuzeigen.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Beispiel

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Aufheben der Zuordnung von Mitgliedskonten in Security Hub CSPM

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Ein AWS Security Hub CSPM-Administratorkonto kann die Zuordnung zu einem Mitgliedskonto aufheben, sodass keine Ergebnisse mehr von diesem Konto empfangen und angezeigt werden. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor Sie es löschen können.

Wenn Sie die Zuordnung zu einem Mitgliedskonto aufheben, verbleibt es in Ihrer Liste der Mitgliedskonten mit dem Status Entfernt (Getrennt). Ihr Konto wird aus den Administratorkontoinformationen für das Mitgliedskonto entfernt.

Um weiterhin Ergebnisse für das Konto zu erhalten, können Sie die Einladung erneut versenden. Um das Mitgliedskonto vollständig zu entfernen, können Sie das Mitgliedskonto löschen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein manuell eingeladenes Mitgliedskonto vom Administratorkonto zu trennen.

Security Hub CSPM console

So trennen Sie die Zuordnung eines manuell eingeladenen Mitgliedskontos

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten.
4. Wählen Sie „Aktionen“ und anschließend „Konto trennen“.

Security Hub CSPM API

Um die Verbindung zu einem manuell eingeladenen Mitgliedskonto zu trennen

Rufen Sie die `DisassociateMembers`API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, deren Zuordnung Sie aufheben möchten. Verwenden Sie den `ListMembers`Vorgang, um eine Liste der Mitgliedskonten anzuzeigen.

AWS CLI

Um die Zuordnung zu einem manuell eingeladenen Mitgliedskonto aufzuheben

Führen Sie den `disassociate-members`Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, deren Zuordnung Sie aufheben möchten. Führen Sie den `list-members`Befehl aus, um eine Liste der Mitgliedskonten anzuzeigen.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Löschen von Mitgliedskonten in Security Hub CSPM

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Als AWS Security Hub CSPM-Administratorkonto können Sie Mitgliedskonten löschen, die auf Einladung hinzugefügt wurden. Bevor Sie ein aktiviertes Konto löschen können, müssen Sie die Verknüpfung mit dem Konto aufheben.

Wenn Sie ein Mitgliedskonto löschen, wird es vollständig aus der Liste entfernt. Um die Mitgliedschaft des Kontos wiederherzustellen, müssen Sie es hinzufügen und erneut einladen, als ob es sich um ein völlig neues Mitgliedskonto handeln würde.

Sie können keine Konten löschen, die zu einer Organisation gehören und die mithilfe der Integration mit verwaltet werdenAWS Organizations.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen manuell eingeladener Mitgliedskonten.

Security Hub CSPM console

Um ein manuell eingeladenes Mitgliedskonto zu löschen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit dem Administratorkonto an.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konfiguration aus.
3. Wählen Sie den Tab Einladungskonten aus. Wählen Sie dann die Konten aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen aus. Diese Option ist nur verfügbar, wenn Sie die Kontoverknüpfung aufgehoben haben. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor es gelöscht werden kann.

Security Hub CSPM API

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Rufen Sie die `DeleteMembers`API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, die Sie löschen möchten. Rufen Sie die `ListMembers`API auf, um die Liste der Mitgliedskonten abzurufen.

AWS CLI

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Führen Sie den `delete-members`Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, die Sie löschen möchten. Führen Sie den `list-members`Befehl aus, um die Liste der Mitgliedskonten abzurufen.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Beispiel

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Trennung von einem Security Hub CSPM-Administratorkonto

> **Note**
>
> Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Wenn Ihr Konto auf Einladung als AWS Security Hub CSPM-Mitgliedskonto hinzugefügt wurde, können Sie die Verbindung zwischen dem Mitgliedskonto und dem Administratorkonto trennen. Nachdem Sie die Zuordnung zu einem Mitgliedskonto aufgehoben haben, sendet Security Hub CSPM keine Ergebnisse aus dem Konto an das Administratorkonto.

Mitgliedskonten, die mithilfe der Integration mit verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur der delegierte Security Hub CSPM-Administrator kann die Zuordnung von Mitgliedskonten aufheben, die mit Organizations verwaltet werden.

Wenn Sie die Verbindung zu Ihrem Administratorkonto trennen, verbleibt Ihr Konto in der Mitgliederliste des Administratorkontos mit dem Status Kündigt. Das Administratorkonto erhält jedoch keine Ergebnisse für Ihr Konto.

Nachdem Sie sich vom Administratorkonto getrennt haben, bleibt die Einladung, Mitglied zu werden, weiterhin bestehen. Sie können die Einladung in future erneut annehmen.

Security Hub CSPM console

Um die Verbindung zu Ihrem Administratorkonto zu trennen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Deaktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Aktualisieren aus.

Security Hub CSPM API

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Rufen Sie die API auf `DisassociateFromAdministratorAccount`.

AWS CLI

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Führen Sie den Befehl `disassociate-from-administrator-account` aus.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Die Security Hub CSPM-Konsole wird weiterhin verwendet. `DisassociateFromMasterAccount` Sie wird irgendwann auf Verwendung umgestellt. `DisassociateFromAdministratorAccount` Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion regeln, müssen weiterhin verwendet `DisassociateFromMasterAccount` werden. Sie sollten Ihre Richtlinien auch ergänzen`DisassociateFromAdministratorAccount`, um sicherzustellen, dass nach

Beginn der Nutzung `DisassociateFromAdministratorAccount` der Konsole die richtigen Berechtigungen vorhanden sind.

Umstellung auf Organizations zur Verwaltung von Konten in Security Hub CSPM

Wenn Sie Konten manuell in AWS Security Hub CSPM verwalten, müssen Sie potenzielle Mitgliedskonten einladen und jedes Mitgliedskonto in jedem Konto separat konfigurieren. AWS-Region

Durch die Integration von Security Hub CSPM und AWS Organizations können Sie das Senden von Einladungen überflüssig machen und mehr Kontrolle darüber gewinnen, wie Security Hub CSPM in Ihrem Unternehmen konfiguriert und angepasst wird. Aus diesem Grund empfehlen wir, AWS Organizations anstelle von Security Hub CSPM-Einladungen zur Verwaltung Ihrer Mitgliedskonten zu verwenden. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations.

Es ist möglich, einen kombinierten Ansatz zu verwenden, bei dem Sie die AWS Organizations Integration verwenden, aber auch Konten außerhalb Ihrer Organisation manuell einladen. Wir empfehlen jedoch, ausschließlich die Organizations-Integration zu verwenden. Die zentrale Konfiguration, eine Funktion, mit der Sie Security Hub CSPM über mehrere Konten und Regionen hinweg verwalten können, ist nur bei der Integration mit Organizations verfügbar.

In diesem Abschnitt wird beschrieben, wie Sie von der manuellen Kontoverwaltung auf Einladungsbasis zur Verwaltung von Konten mit übergehen können. AWS Organizations

Integration von Security Hub CSPM mitAWS Organizations

Zunächst müssen Sie Security Hub CSPM und integrieren. AWS Organizations

Sie können diese Dienste integrieren, indem Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Organisation inAWS Organizations. Anweisungen finden Sie im AWS OrganizationsBenutzerhandbuch unter Organisation erstellen.
- Geben Sie im Verwaltungskonto Organizations ein delegiertes Security Hub-CSPM-Administratorkonto an.

> **Note**
>
> Das Organisationsverwaltungskonto kann nicht als DA-Konto festgelegt werden.

Detaillierte Anweisungen finden Sie unter Integration von Security Hub CSPM mitAWS Organizations.

Indem Sie die vorherigen Schritte ausführen, gewähren Sie vertrauenswürdigen Zugriff für Security Hub CSPM in. AWS Organizations Dadurch wird auch Security Hub CSPM in der aktuellen Version AWS-Region für das delegierte Administratorkonto aktiviert.

Der delegierte Administrator kann die Organisation in Security Hub CSPM verwalten, indem er in erster Linie die Konten der Organisation als Security Hub CSPM-Mitgliedskonten hinzufügt. Der Administrator kann auch auf bestimmte Security Hub CSPM-Einstellungen, Daten und Ressourcen für diese Konten zugreifen.

Wenn Sie zur Kontoverwaltung mit Organizations wechseln, werden Konten, die auf Einladung basieren, nicht automatisch zu Security Hub CSPM-Mitgliedern. Nur die Konten, die Sie zu Ihrer neuen Organisation hinzufügen, können Security Hub CSPM-Mitglieder werden.

Nach der Aktivierung der Integration können Sie Konten bei Organizations verwalten. Weitere Informationen finden Sie unter Security Hub CSPM für mehrere Konten verwalten mitAWS Organizations. Die Kontoverwaltung variiert je nach Konfigurationstyp Ihrer Organisation.

Zulässige Aktionen von Administrator- und Mitgliedskonten in Security Hub CSPM

Administrator- und Mitgliedskonten haben Zugriff auf die in den folgenden Tabellen aufgeführten AWS Security Hub CSPM-Aktionen. In den Tabellen haben die Werte die folgenden Bedeutungen:

- Beliebig — Das Konto kann die Aktion für jedes Mitgliedskonto unter demselben Administrator ausführen.
- Aktuell — Das Konto kann die Aktion nur für sich selbst ausführen (das Konto, bei dem Sie derzeit angemeldet sind).
- Dash — Zeigt an, dass das Konto die Aktion nicht ausführen kann.

Wie in den Tabellen angegeben, hängen die zulässigen Aktionen davon ab, ob Sie eine Integration vornehmen AWS Organizations und welchen Konfigurationstyp Ihre Organisation verwendet.

Informationen zum Unterschied zwischen zentraler und lokaler Konfiguration finden Sie unterKonten verwalten mitAWS Organizations.

Security Hub CSPM kopiert die Ergebnisse des Mitgliedskontos nicht in das Administratorkonto. In Security Hub CSPM werden alle Ergebnisse für ein bestimmtes Konto in einer bestimmten Region erfasst. In jeder Region kann das Administratorkonto die Ergebnisse für seine Mitgliedskonten in dieser Region einsehen und verwalten.

Wenn Sie eine Aggregationsregion festlegen, kann das Administratorkonto die Ergebnisse von Mitgliedskonten aus verknüpften Regionen anzeigen und verwalten, die in die Aggregationsregion repliziert werden. Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter Aggregation. Cross-Region

In den folgenden Tabellen werden die Standardberechtigungen für Administrator- und Mitgliedskonten angegeben. Sie können benutzerdefinierte IAM-Richtlinien verwenden, um den Zugriff auf die Features und Funktionen von Security Hub CSPM weiter einzuschränken. Anleitungen und Beispiele finden Sie im Blogbeitrag Aligning IAM-Policies to user personas for AWS Security Hub CSPM.

Zulässige Aktionen, wenn Sie in Organizations integrieren und die zentrale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie eine Integration mit Organizations durchführen und die zentrale Konfiguration verwenden.

Action	Delegiertes Security Hub-CSPM-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Self-managed Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	Für selbst und zentral verwaltete Konten	–	–
Organisationskonten anzeigen	Beliebig	–	–
Mitgliedskonto trennen	Beliebig	–	–

Action	Delegiertes Security Hub-CSPM-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Self-managed Mitgliedskonto
Mitgliedskonto löschen	Jedes Konto, das nicht zur Organisation gehört	–	–
Security Hub CSPM deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell (muss vom Administratorkonto getrennt werden)
Ergebnisse und Fundverlauf anzeigen	Beliebig	Aktuell	Aktuell
Ergebnisse aktualisieren	Beliebig	Aktuell	Aktuell
Insight-Ergebnisse anzeigen	Beliebig	Aktuell	Aktuell
Kontrolldetails anzeigen	Beliebig	Aktuell	Aktuell
Schalten Sie konsolidierte Kontrolle rgebnisse ein oder aus	Beliebig	–	–
Aktivieren und deaktivieren Sie Standards	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Steuerungen aktivieren und deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Integrationen aktivieren und deaktivieren	Aktuell	Aktuell	Aktuell

Action	Delegiertes Security Hub-CSPM-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Self-managed Mitgliedskonto
Konfigurieren Sie die regionsübergreifende Aggregation	Beliebig	–	–
Wählen Sie die Heimatregion und die verknüpften Regionen	Beliebig (Sie müssen die zentrale Konfiguration beenden und neu starten, um die Heimatregion zu ändern)	–	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Beliebig	–	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell	Aktuell

Zulässige Aktionen, wenn Sie eine Integration mit Organizations durchführen und die lokale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie eine Integration mit Organizations durchführen und die lokale Konfiguration verwenden.

Action	Delegiertes Security Hub-CSPM-Administratorkonto	Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Beliebig	–
Mitgliedskonto trennen	Beliebig	–
Mitgliedskonto löschen	–	–
Security Hub CSPM deaktivieren	–	Aktuell (wenn das Konto vom delegierten Administrator getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Beliebig	Aktuell
Ergebnisse aktualisieren	Beliebig	Aktuell
Insight-Ergebnisse anzeigen	Beliebig	Aktuell
Kontrolldetails anzeigen	Beliebig	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Beliebig	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell
Automatisches Aktivieren von Security Hub CSPM und Standardstandards in neuen Unternehmenskonten	Für Girokonten und neue Organisationskonten	–

Action	Delegiertes Security Hub-CSPM-Administratorkonto	Mitgliedskonto
Steuerelemente aktivieren und deaktivieren	Aktuell	Aktuell
Aktiviere und deaktiviere Integrationen	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Beliebig	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Beliebig	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell

Zulässige Aktionen für Konten, die auf Einladungen basieren

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie die einladungsbasierte Methode verwenden, um Konten manuell zu verwalten, anstatt sie zu integrieren. AWS Organizations

Action	Security Hub CSPM-Administratorkonto	Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Beliebig	–
Mitgliedskonto trennen	Beliebig	Aktuell

Action	Security Hub CSPM-Administratorkonto	Mitgliedskonto
Mitgliedskonto löschen	Beliebig	–
Security Hub CSPM deaktivieren	Aktuell (wenn keine aktivierten Mitgliedskonten vorhanden sind)	Aktuell (wenn das Konto vom Administratorkonto getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Beliebig	Aktuell
Ergebnisse aktualisieren	Beliebig	Aktuell
Insight-Ergebnisse anzeigen	Beliebig	Aktuell
Kontrolldetails anzeigen	Beliebig	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Beliebig	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell
Automatisches Aktivieren von Security Hub CSPM und Standardstandards in neuen Unternehmenskonten	–	–
Steuerungen aktivieren und deaktivieren	Aktuell	Aktuell
Aktiviere und deaktiviere Integrationen	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Beliebig	–

Action	Security Hub CSPM-Administratorkonto	Mitgliedskonto
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Beliebig	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell

Auswirkung von Kontoaktionen auf Security Hub CSPM-Daten

Diese Kontoaktionen haben die folgenden Auswirkungen auf die AWS Security Hub CSPM-Daten.

Security Hub CSPM deaktiviert

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator (DA) Security Hub CSPM-Konfigurationsrichtlinien erstellen, die AWS Security Hub CSPM in bestimmten Konten und Organisationseinheiten (OUs) deaktivieren. In diesem Fall ist Security Hub CSPM in den angegebenen Konten und Organisationseinheiten in Ihrer Heimatregion und allen verknüpften Regionen deaktiviert. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub CSPM in jedem Konto und jeder Region, in der Sie es aktiviert haben, separat deaktivieren. Sie können die zentrale Konfiguration nicht verwenden, wenn Security Hub CSPM im DA-Konto deaktiviert ist.

Für das Administratorkonto werden keine Ergebnisse generiert oder aktualisiert, wenn Security Hub CSPM im Administratorkonto deaktiviert ist. Bestehende archivierte Ergebnisse werden nach 30 Tagen gelöscht. Bestehende aktive Ergebnisse werden nach 90 Tagen gelöscht.

Integrationen mit anderen AWS-Services werden entfernt.

Aktivierte Sicherheitsstandards und Kontrollen sind deaktiviert.

Andere Security Hub CSPM-Daten und -Einstellungen, einschließlich benutzerdefinierter Aktionen, Einblicke und Abonnements für Produkte von Drittanbietern, werden 90 Tage lang aufbewahrt.

Das Mitgliedskonto wurde vom Administratorkonto getrennt

Wenn die Verknüpfung eines Mitgliedskontos mit dem Administratorkonto getrennt wird, verliert das Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub CSPM ist jedoch weiterhin in beiden Konten aktiviert.

Wenn Sie die zentrale Konfiguration verwenden, kann der DA Security Hub CSPM nicht für ein Mitgliedskonto konfigurieren, das vom DA-Konto getrennt ist.

Benutzerdefinierte Einstellungen oder Integrationen, die für das Administratorkonto definiert sind, werden nicht auf Ergebnisse aus dem früheren Mitgliedskonto angewendet. Wenn die Konten beispielsweise getrennt wurden, haben Sie möglicherweise eine benutzerdefinierte Aktion im Administratorkonto, die als Ereignismuster in einer EventBridge Amazon-Regel verwendet wird. Diese benutzerdefinierte Aktion kann jedoch nicht im Mitgliedskonto verwendet werden.

In der Kontenliste für das Security Hub CSPM-Administratorkonto hat ein entferntes Konto den Status Getrennt.

Das Mitgliedskonto wurde aus einer Organisation entfernt

Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, verliert das Security Hub CSPM-Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub CSPM ist jedoch weiterhin in beiden Konten mit denselben Einstellungen aktiviert, die sie vor dem Entfernen hatten.

Wenn Sie die zentrale Konfiguration verwenden, können Sie Security Hub CSPM nicht für ein Mitgliedskonto konfigurieren, nachdem es aus der Organisation entfernt wurde, zu der der delegierte Administrator gehört. Das Konto behält jedoch die Einstellungen bei, die es vor der Entfernung hatte, sofern Sie sie nicht manuell ändern.

In der Kontenliste für das Security Hub CSPM-Administratorkonto hat ein entferntes Konto den Status Gelöscht.

Das Konto ist gesperrt

Wenn ein gesperrt AWS-Konto wird, verliert das Konto die Erlaubnis, seine Ergebnisse in Security Hub CSPM einzusehen. Für dieses Konto werden keine Ergebnisse generiert oder aktualisiert. Das Administratorkonto für ein gesperrtes Konto kann die vorhandenen Ergebnisse für das Konto einsehen.

Bei einem Unternehmenskonto kann sich der Status des Mitgliedskontos auch in Konto gesperrt ändern. Dies ist der Fall, wenn das Konto gleichzeitig gesperrt wird, während das Administratorkonto versucht, das Konto zu aktivieren. Das Administratorkonto für ein gesperrtes Konto kann die Ergebnisse für dieses Konto nicht einsehen. Andernfalls hat der Status „Gesperrt“ keinen Einfluss auf den Status des Mitgliedskontos.

Wenn Sie die zentrale Konfiguration verwenden, schlägt die Richtlinienzuweisung fehl, wenn der delegierte Administrator versucht, einem gesperrten Konto eine Konfigurationsrichtlinie zuzuordnen.

Nach 90 Tagen wird das Konto entweder gekündigt oder reaktiviert. Wenn das Konto reaktiviert wird, werden seine Security Hub CSPM-Berechtigungen wiederhergestellt. Wenn das Mitgliedskonto den Status Konto gesperrt hat, muss das Administratorkonto das Konto manuell aktivieren.

Das Konto ist geschlossen

Wenn ein geschlossen AWS-Konto wird, reagiert Security Hub CSPM wie folgt auf das Schließen.

Wenn es sich bei dem Konto um ein Security Hub CSPM-Administratorkonto handelt, wird es als Administratorkonto entfernt und alle Mitgliedskonten werden entfernt. Wenn es sich bei dem Konto um ein Mitgliedskonto handelt, wird es getrennt und als Mitglied aus dem Security Hub CSPM-Administratorkonto entfernt.

Security Hub CSPM bewahrt bestehende archivierte Ergebnisse 30 Tage lang im Konto auf. Bei einem Kontrollbefund basiert die Berechnung von 30 Tagen auf dem Wert für das `UpdatedAt` Feld, in dem das Ergebnis festgestellt wurde. Bei einem anderen Befundtyp basiert die Berechnung auf dem Wert für das `ProcessedAt` Feld `UpdatedAt` oder des Ergebnisses, je nachdem, welches Datum das späteste ist. Nach Ablauf dieser 30-tägigen Frist löscht Security Hub CSPM den Befund dauerhaft aus dem Konto.

Security Hub CSPM speichert bestehende aktive Ergebnisse 90 Tage lang im Konto. Bei einem Kontrollbefund basiert die Berechnung von 90 Tagen auf dem Wert für das `UpdatedAt` Feld, in dem das Ergebnis festgestellt wurde. Bei einem anderen Befundtyp basiert die Berechnung auf dem Wert für das `ProcessedAt` Feld `UpdatedAt` oder des Ergebnisses, je nachdem, welches Datum das späteste ist. Am Ende dieses 90-Tage-Zeitraums löscht Security Hub CSPM den Befund dauerhaft aus dem Konto.

Zur längerfristigen Aufbewahrung vorhandener Ergebnisse können Sie die Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter Verwendung EventBridge für automatische Reaktionen und Problembehebungen.

> **Important**
>
> Für Kunden, die sich angemeldet habenAWS GovCloud (US) Regions, erstellen Sie eine Sicherungskopie und löschen Sie dann Ihre Versicherungsdaten und andere Kontoressourcen, bevor Sie Ihr Konto schließen. Nachdem Sie Ihr Konto geschlossen haben, haben Sie keinen Zugriff mehr auf die Ressourcen und Daten.

Weitere Informationen finden Sie unter Schließen und AWS-Konto im AWS - KontenverwaltungReferenzhandbuch.

Grundlegendes zur regionsübergreifenden Aggregation in Security Hub CSPM

> **Note**
>
> Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Durch die Verwendung der regionsübergreifenden Aggregation in AWS Security Hub CSPM können Sie Ergebnisse zusammenfassen, Updates und Erkenntnisse finden, den Compliance-Status und Sicherheitsbewertungen von mehreren AWS-Regionen zu einer einzigen Heimatregion kontrollieren. Anschließend können Sie all diese Daten von der Heimatregion aus verwalten.

Angenommen, Sie legen USA Ost (Nord-Virginia) als Heimatregion und USA West (Oregon) und USA West (Nordkalifornien) als verknüpfte Regionen fest. Wenn Sie die Ergebnisseite in USA Ost (Nord-Virginia) aufrufen, sehen Sie die Ergebnisse aus allen drei Regionen. Aktualisierungen dieser Ergebnisse spiegeln sich auch in allen drei Regionen wider.

> **Note**
>
> In AWS GovCloud (US) wird die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Erkenntnisse in allen Regionen unterstützt. AWS GovCloud (US) Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen AWS GovCloud (US-East) und AWS GovCloud (US-West) aggregieren. In den Regionen China wird die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen

und Erkenntnisse in den Regionen China unterstützt. Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen China (Peking) und China (Ningxia) zusammenfassen.

Wenn ein Steuerelement in einer verknüpften Region aktiviert, aber in der Heimatregion deaktiviert ist, können Sie den Konformitätsstatus des Steuerelements in der Heimatregion anzeigen, aber Sie können dieses Steuerelement nicht von der Heimatregion aus aktivieren oder deaktivieren. Die Ausnahme ist, wenn Sie die zentrale Konfiguration verwenden. Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Security Hub CSPM-Administrator Steuerungen in der Heimatregion und verknüpften Regionen von der Heimatregion aus konfigurieren.

Wenn Sie eine Heimatregion festgelegt haben, berücksichtigen die Sicherheitswerte den Kontrollstatus in allen verknüpfte Regionen. Um regionsübergreifende Sicherheitsbewertungen und Compliance-Status anzuzeigen, fügen Sie Ihrer IAM-Rolle, die Security Hub CSPM verwendet, die folgenden Berechtigungen hinzu:

- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

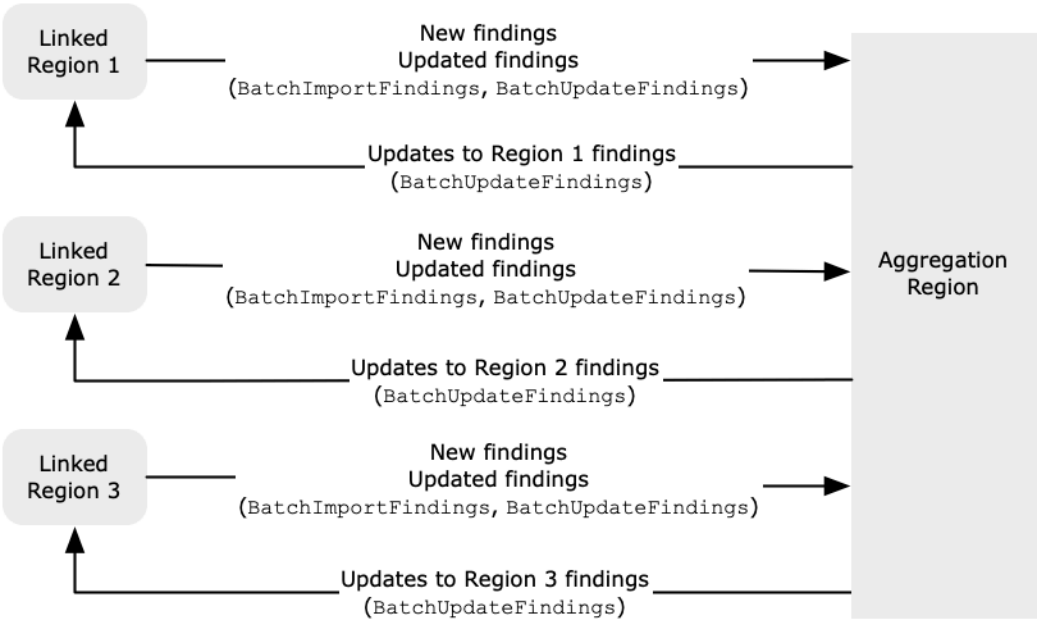
Arten von Daten, die aggregiert sind

Wenn die regionsübergreifende Aggregation mit einer oder mehreren verknüpften Regionen aktiviert ist, repliziert Security Hub CSPM die folgenden Daten aus den verknüpften Regionen in die Heimatregion. Dies geschieht in jedem Konto, für das die regionsübergreifende Aggregation aktiviert ist.

- Ergebnisse
- Insights
- Kontrollieren Sie den Compliance-Status
- Sicherheitswerte

Zusätzlich zu den neuen Daten in der vorherigen Liste repliziert Security Hub CSPM auch Aktualisierungen dieser Daten zwischen den verknüpften Regionen und der Heimatregion. Updates, die in einer verknüpften Region vorgenommen werden, werden in die Heimatregion repliziert.

Aktualisierungen, die in der Heimatregion vorgenommen werden, werden zurück in die verknüpfte Region repliziert. Wenn es in der Heimatregion und der verknüpften Region widersprüchliche Aktualisierungen gibt, wird das neueste Update verwendet.



Cross-Region Die Aggregation erhöht nicht die Kosten von Security Hub CSPM. Es fallen keine Gebühren an, wenn Security Hub CSPM neue Daten oder Updates repliziert.

In der Heimatregion bietet die Übersichtsseite einen Überblick über Ihre aktiven Ergebnisse in den verknüpften Regionen. Weitere Informationen finden Sie unter Eine regionsübergreifende Zusammenfassung der Ergebnisse nach Schweregrad anzeigen. In anderen Bereichen auf der Übersichtsseite, in denen Ergebnisse analysiert werden, werden ebenfalls Informationen aus allen verknüpften Regionen angezeigt.

Ihre Sicherheitswerte in der Heimatregion werden berechnet, indem die Anzahl der bestandenen Kontrollen mit der Anzahl der aktivierten Kontrollen in allen verknüpften Regionen verglichen wird. Wenn ein Steuerelement in mindestens einer verknüpften Region aktiviert ist, ist es außerdem auf den Detailseiten zu den Sicherheitsstandards der Heimatregion sichtbar. Der Konformitätsstatus der Kontrollen auf den Seiten mit den Standarddetails spiegelt die Ergebnisse der einzelnen verknüpften Regionen wider. Wenn eine mit einer Kontrolle verknüpfte Sicherheitsüberprüfung in einer oder mehreren verknüpften Regionen fehlschlägt, wird der Konformitätsstatus dieser Kontrolle auf den Standarddetailseiten der Heimatregion als Fehlgeschlagen angezeigt. Die Anzahl der Sicherheitsüberprüfungen umfasst Ergebnisse aus allen verknüpften Regionen.

Security Hub CSPM aggregiert nur Daten aus Regionen, in denen Security Hub CSPM für ein Konto aktiviert ist. Security Hub CSPM wird nicht automatisch für ein Konto aktiviert, das auf der regionsübergreifenden Aggregationskonfiguration basiert.

Es ist möglich, die regionsübergreifende Aggregation zu aktivieren, ohne dass verknüpfte Regionen ausgewählt werden. In diesem Fall findet keine Datenreplikation statt.

Aggregation für Administrator- und Mitgliedskonten

Eigenständige Konten, Mitgliedskonten und Administratorkonten können die regionsübergreifende Aggregation konfigurieren. Falls von einem Administrator konfiguriert, ist das Vorhandensein des Administratorkontos unerlässlich, damit die regionsübergreifende Aggregation in verwalteten Konten funktioniert. Wenn das Administratorkonto entfernt oder von einem Mitgliedskonto getrennt wird, wird die regionsübergreifende Aggregation für das Mitgliedskonto beendet. Dies gilt auch dann, wenn für das Konto die regionsübergreifende Aggregation aktiviert war, bevor die Beziehung zwischen Administrator und Mitglied aufgenommen wurde.

Wenn ein Administratorkonto die regionsübergreifende Aggregation aktiviert, repliziert Security Hub CSPM die Daten, die das Administratorkonto in allen verknüpften Regionen generiert, in die Heimatregion. Darüber hinaus identifiziert Security Hub CSPM die Mitgliedskonten, die diesem Administrator zugeordnet sind, und jedes Mitgliedskonto erbt die regionsübergreifenden Aggregationseinstellungen des Administrators. Security Hub CSPM repliziert die Daten, die ein Mitgliedskonto in allen verknüpften Regionen generiert, in die Heimatregion.

Der Administrator kann von allen Mitgliedskonten in den verwalteten Regionen aus auf Sicherheitsergebnisse zugreifen und diese verwalten. Als Security Hub CSPM-Administrator müssen Sie jedoch in der Heimatregion angemeldet sein, um aggregierte Daten aus allen Mitgliedskonten und verknüpften Regionen einsehen zu können.

Als Security Hub CSPM-Mitgliedskonto müssen Sie in der Heimatregion angemeldet sein, um aggregierte Daten aus Ihrem Konto aus allen verknüpften Regionen einsehen zu können. Mitgliedskonten sind nicht berechtigt, Daten von anderen Mitgliedskonten einzusehen.

Ein Administratorkonto kann Mitgliedskonten manuell einladen oder als delegierter Administrator einer Organisation fungieren, in die integriert AWS Organizations ist. Bei einem Mitgliedskonto mit manueller Einladung muss der Administrator das Konto aus der Heimatregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss für das Mitgliedskonto Security Hub CSPM in der Heimatregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann. Wenn Sie

die Heimatregion nicht für andere Zwecke verwenden, können Sie die Security Hub CSPM-Standards und -Integrationen in dieser Region deaktivieren, um Gebühren zu vermeiden.

Wenn Sie die regionsübergreifende Aggregation verwenden möchten und über mehrere Administratorkonten verfügen, empfehlen wir Ihnen, die folgenden bewährten Methoden zu befolgen:

- Jedes Administratorkonto hat unterschiedliche Mitgliedskonten.
- Jedes Administratorkonto hat in allen Regionen dieselben Mitgliedskonten.
- Jedes Administratorkonto verwendet eine andere Heimatregion.

> **Note**
>
> Informationen darüber, wie sich die regionsübergreifende Aggregation auf die zentrale Konfiguration auswirkt, finden Sie unter. Auswirkungen der zentralen Konfiguration auf die regionsübergreifende Aggregation

Auswirkungen der zentralen Konfiguration auf die regionsübergreifende Aggregation

Die zentrale Konfiguration ist eine optionale Funktion in AWS Security Hub CSPM, die Sie verwenden können, wenn Sie sie integrieren. AWS Organizations Wenn Sie die zentrale Konfiguration verwenden, kann das delegierte Administratorkonto den Security Hub CSPM-Dienst, die Standards und Kontrollen für Konten und Organisationseinheiten (OU) in der Organisation konfigurieren. Um Konten und Organisationseinheiten zu konfigurieren, erstellt der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann definiert werden, ob Security Hub CSPM aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert sind. Der delegierte Administrator ordnet Konfigurationsrichtlinien bestimmten Konten, Organisationseinheiten oder dem Stamm (der gesamten Organisation) zu.

Der delegierte Administrator kann Konfigurationsrichtlinien für die Organisation nur von der Heimatregion aus erstellen und verwalten. Darüber hinaus werden Konfigurationsrichtlinien in der Heimatregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur für einige verknüpfte Regionen gilt und nicht für andere. Informationen zur regionsübergreifenden Aggregation finden Sie unter Cross-Region Aggregation.

Um die zentrale Konfiguration verwenden zu können, müssen Sie eine Heimatregion angeben. Optional können Sie eine oder mehrere Regionen als verknüpfte Regionen auswählen. Sie können sich auch dafür entscheiden, eine Heimatregion ohne verknüpfte Regionen festzulegen.

Eine Änderung Ihrer regionsübergreifenden Aggregationseinstellungen kann sich auf Ihre Konfigurationsrichtlinien auswirken. Wenn Sie eine verknüpfte Region hinzufügen, werden Ihre Konfigurationsrichtlinien in dieser Region wirksam. Wenn es sich bei der Region um eine Opt-in-Region handelt, muss die Region aktiviert sein, damit Ihre Konfigurationsrichtlinien dort wirksam werden. Umgekehrt sind die Konfigurationsrichtlinien in dieser Region nicht mehr wirksam, wenn Sie eine verknüpfte Region entfernen. In dieser Region behalten die Konten die Einstellungen bei, die sie hatten, als die verknüpfte Region entfernt wurde. Sie können diese Einstellungen ändern, müssen dies jedoch für jedes Konto und jede Region separat tun.

Wenn Sie die Heimatregion entfernen oder ändern, werden Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen gelöscht. Sie können in keiner Region mehr die zentrale Konfiguration verwenden oder Konfigurationsrichtlinien erstellen. Konten behalten die Einstellungen bei, die sie hatten, bevor die Heimatregion geändert oder entfernt wurde. Sie können diese Einstellungen jederzeit ändern. Da Sie die zentrale Konfiguration jedoch nicht mehr verwenden, müssen die Einstellungen für jedes Konto und jede Region separat geändert werden. Sie können die zentrale Konfiguration verwenden und erneut Konfigurationsrichtlinien erstellen, wenn Sie eine neue Heimatregion angeben.

Weitere Informationen zur zentralen Konfiguration finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Aktivierung der regionsübergreifenden Aggregation

> **Note**
>
> Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie müssen die regionsübergreifende Aggregation von der Region aus aktivierenAWS-Region, die Sie als Heimatregion festlegen möchten.

Um die regionsübergreifende Aggregation zu aktivieren, erstellen Sie eine Security Hub-CSPM-Ressource, die als Finding-Aggregator bezeichnet wird. Die Suchaggregator-Ressource gibt Ihre Heimatregion und verknüpfte Regionen (falls vorhanden) an.

Sie können keine RegionAWS-Region, die standardmäßig deaktiviert ist, als Heimatregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie unter Aktivieren einer Region in der Allgemeine AWS-Referenz.

Wenn Sie die regionsübergreifende Aggregation aktivieren, können Sie bei Bedarf eine oder mehrere verknüpfte Regionen angeben. Sie können auch wählen, ob neue Regionen automatisch verknüpft werden sollen, wenn Security Hub CSPM sie zu unterstützen beginnt und Sie sich für sie entschieden haben.

Security Hub CSPM console

Um die regionsübergreifende Aggregation zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Melden Sie sich mit dem AWS-Region Selektor bei der Region an, die Sie als Aggregationsregion verwenden möchten.
3. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Suchaggregation die Option Suchaggregation konfigurieren aus.

   Standardmäßig ist die Heimatregion auf Keine Aggregationsregion gesetzt.
5. Wählen Sie unter Aggregationsregion die Option aus, um die aktuelle Region als Heimatregion festzulegen.
6. Wählen Sie optional für Verknüpfte Regionen die Regionen aus, aus denen Daten aggregiert werden sollen.
7. Um Daten aus neuen Regionen in der Partition automatisch zu aggregieren, sofern Security Hub CSPM sie unterstützt und Sie sich für sie entscheiden, wählen Sie future Regionen verknüpfen aus.
8. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie von der Region aus, die Sie als Heimatregion verwenden möchten, den `CreateFindingAggregator`Betrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl create-finding-aggregator aus.

Wählen Sie unter `RegionLinkingMode` eine der folgenden Optionen aus:

- `ALL_REGIONS`— Security Hub CSPM aggregiert Daten aus allen Regionen. Security Hub CSPM aggregiert auch Daten aus neuen Regionen, sobald diese unterstützt werden und Sie sich für sie entscheiden.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub CSPM aggregiert Daten aus allen Regionen mit Ausnahme der Regionen, die Sie ausschließen möchten. Security Hub CSPM aggregiert auch Daten aus neuen Regionen, sobald diese unterstützt werden und Sie sich für sie entscheiden. Dient `Regions` zur Bereitstellung der Liste der Regionen, die von der Aggregation ausgeschlossen werden sollen.
- `SPECIFIED_REGIONS`— Security Hub CSPM aggregiert Daten aus einer ausgewählten Liste von Regionen. Security Hub CSPM aggregiert Daten aus neuen Regionen nicht automatisch. Wird verwendet`Regions`, um die Liste der Regionen bereitzustellen, aus denen aggregiert werden soll.
- `NO_REGIONS`— Security Hub CSPM aggregiert keine Daten, da Sie keine verknüpften Regionen auswählen.

Im folgenden Beispiel wird die regionsübergreifende Aggregation konfiguriert. Die Heimatregion ist USA Ost (Nord-Virginia). Die verbundenen Regionen sind USA West (Nordkalifornien) und USA West (Oregon). Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Überprüfung der Einstellungen für die regionsübergreifende Aggregation

> **Note**
>
> Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie können die aktuelle regionsübergreifende Aggregationskonfiguration in AWS Security Hub CSPM von jedem aus anzeigen. AWS-Region Die Konfiguration umfasst die Heimatregion, die verknüpften Regionen (falls vorhanden) und ob neue Regionen automatisch verknüpft werden sollen, da Security Hub CSPM sie unterstützt.

Mitgliedskonten können die regionsübergreifenden Aggregationseinstellungen einsehen, die das Administratorkonto konfiguriert hat.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre aktuellen regionsübergreifenden Aggregationseinstellungen anzuzeigen.

Security Hub CSPM console

So zeigen Sie regionsübergreifende Aggregationseinstellungen an (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Regionen.

Wenn die regionsübergreifende Aggregation nicht aktiviert ist, wird auf der Registerkarte Regionen die Option zur Aktivierung der regionsübergreifenden Aggregation angezeigt. Nur Administratorkonten und eigenständige Konten können die regionsübergreifende Aggregation aktivieren.

Wenn die regionsübergreifende Aggregation aktiviert ist, werden auf der Registerkarte Regionen die folgenden Informationen angezeigt:

- Die Heimatregion
- Ob Ergebnisse, Erkenntnisse, Kontrollstatus und Sicherheitswerte aus neuen Regionen, die Security Hub CSPM unterstützt und für die Sie sich entscheiden, automatisch aggregiert werden sollen
- Die Liste der verknüpften Regionen (falls welche ausgewählt wurden)

Security Hub CSPM API

So überprüfen Sie die Einstellungen für die regionsübergreifende Aggregation (Security Hub CSPM API)

Verwenden Sie den `GetFindingAggregator`Betrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl get-finding-aggregator aus.

Wenn Sie die Anfrage stellen, geben Sie den Suchaggregator-ARN an. Verwenden Sie den Befehl `ListFindingAggregators`operation oder list-finding-aggregators, um den Finding-Aggregator-ARN abzurufen.

Das folgende Beispiel zeigt die regionsübergreifenden Aggregationseinstellungen für den angegebenen Suchaggregator-ARN. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Aktualisierung der regionsübergreifenden Aggregationseinstellungen

> **Note**
>
> Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie können Ihre aktuellen regionsübergreifenden Aggregationseinstellungen in AWS Security Hub CSPM aktualisieren, indem Sie die verknüpften Regionen oder die aktuelle Heimatregion ändern. Sie können auch ändern, ob Daten aus neuen Dateien, in AWS-Regionen denen Security Hub CSPM unterstützt wird, automatisch aggregiert werden sollen.

Änderungen an der regionsübergreifenden Aggregation werden für eine Opt-in-Region erst implementiert, wenn Sie die Region in Ihrer aktivieren. AWS-Konto Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, sind Opt-in-Regionen.

Wenn Sie die Aggregation von Daten aus einer verknüpften Region beenden, entfernt AWS Security Hub CSPM keine vorhandenen aggregierten Daten aus dieser Region, auf die in der Heimatregion zugegriffen werden kann.

Sie können die Aktualisierungsverfahren in diesem Abschnitt nicht verwenden, um die Heimatregion zu ändern. Um die Heimatregion zu ändern, müssen Sie wie folgt vorgehen:

1. Beenden Sie die regionsübergreifende Aggregation. Detaillierte Anweisungen finden Sie unter the section called “Die Aggregation wird beendet”.
2. Wechseln Sie zu der Region, die Sie als neue Heimatregion verwenden möchten.
3. Aktivieren Sie die regionsübergreifende Aggregation. Detaillierte Anweisungen finden Sie unter the section called “Aggregation aktivieren”.

Sie müssen die regionsübergreifende Aggregationskonfiguration von der aktuellen Heimatregion aus aktualisieren.

Security Hub CSPM console

Um die verknüpften Regionen zu ändern

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich bei der aktuellen Aggregationsregion an.
2. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
3. Wählen Sie für Finding Aggregation die Option Bearbeiten aus.
4. Aktualisieren Sie für verknüpfte Regionen die ausgewählten verknüpften Regionen.
5. Ändern Sie bei Bedarf, ob die Option future Regionen verknüpfen ausgewählt ist. Diese Einstellung bestimmt, ob Security Hub CSPM neue Regionen automatisch verknüpft, wenn es Unterstützung für sie hinzufügt und Sie sich für sie entscheiden.
6. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie die Operation `UpdateFindingAggregator`. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl update-finding-aggregator aus. Um den Suchaggregator zu identifizieren, müssen Sie den Suchaggregator-ARN angeben. Verwenden Sie den Befehl `ListFindingAggregators`operation oder list-finding-aggregators, um den ARN des Finding-Aggregators abzurufen.

Wenn der Linkmodus `ALL_REGIONS_EXCEPT_SPECIFIED` oder ist`SPECIFIED_REGIONS`, können Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern. Wenn Sie den Modus für die Verknüpfung von Regionen auf ändern möchten`NO_REGIONS`, sollten Sie keine Regionenliste angeben.

Wenn Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern, müssen Sie die vollständige Liste zusammen mit den Aktualisierungen bereitstellen. Angenommen, Sie aggregieren derzeit Ergebnisse aus USA Ost (Ohio) und möchten auch Ergebnisse aus USA West (Oregon) aggregieren. Sie müssen eine `Regions` Liste bereitstellen, die sowohl USA Ost (Ohio) als auch USA West (Oregon) enthält.

Im folgenden Beispiel wird die regionsübergreifende Aggregation für ausgewählte Regionen aktualisiert. Der Befehl wird von der aktuellen Heimatregion aus ausgeführt, die USA Ost (Nord-Virginia) ist. Die verknüpften Regionen sind USA West (Nordkalifornien) und USA West (Oregon). Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Die regionsübergreifende Aggregation wird beendet

> **Note**
>
> Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Wenn Sie nicht möchten, dass AWS Security Hub CSPM Daten aggregiert, können Sie Ihren Finding-Aggregator löschen. Alternativ können Sie Ihren Suchaggregator beibehalten, aber keinen mit der Heimatregion verknüpfenAWS-Regionen, indem Sie den vorhandenen Aggregator auf den Verbindungsmodus aktualisieren. `NO_REGIONS`

Um Ihre Heimatregion zu ändern, müssen Sie Ihren aktuellen Suchaggregator löschen und einen neuen erstellen.

Wenn Sie Ihren Suchaggregator löschen, beendet Security Hub CSPM die Datenaggregation. Es entfernt keine vorhandenen aggregierten Daten aus der Heimatregion.

Der Suchaggregator (Konsole) wird gelöscht

Sie können Ihren Suchaggregator nur aus der aktuellen Heimatregion löschen.

In anderen Regionen als der Heimatregion wird im Bereich Finding Aggregation auf der Security Hub CSPM-Konsole eine Meldung angezeigt, dass Sie die Konfiguration in der Heimatregion bearbeiten müssen. Wählen Sie diese Nachricht, um einen Link anzuzeigen, über den Sie zur Heimatregion wechseln können.

Security Hub CSPM console

Um die regionsübergreifende Aggregation zu beenden (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Stellen Sie sicher, dass Sie in Ihrer aktuellen Heimatregion angemeldet sind.
3. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Aggregation suchen die Option Bearbeiten aus.
5. Wählen Sie unter Aggregationsregion die Option Keine Aggregationsregion aus.
6. Wählen Sie Speichern.
7. Geben Sie im Bestätigungsdialogfeld in das Bestätigungsfeld Folgendes ein. **`Confirm`**
8. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Verwenden Sie den `DeleteFindingAggregator`Betrieb der Security Hub CSPM-API. Wenn Sie den verwendenAWS CLI, führen Sie den `delete-finding-aggregator`Befehl aus.

Um den Suchaggregator zu identifizieren, der gelöscht werden soll, geben Sie den Suchaggregator-ARN an. Verwenden Sie die `ListFindingAggregators`Operation oder den `list-finding-aggregators`Befehl, um den Suchaggregator-ARN abzurufen.

Im folgenden Beispiel wird der Suchaggregator gelöscht. Der Befehl wird von der aktuellen Heimatregion aus ausgeführt, die USA Ost (Nord-Virginia) ist. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region us-east-1
```

Sicherheitsstandards in Security Hub CSPM verstehen

In AWS Security Hub CSPM besteht ein Sicherheitsstandard aus einer Reihe von Anforderungen, die auf regulatorischen Rahmenbedingungen, branchenüblichen Best Practices oder

Unternehmensrichtlinien basieren. Einzelheiten zu den Standards, die Security Hub CSPM derzeit unterstützt, einschließlich der Sicherheitskontrollen, die für jeden Standard gelten, finden Sie unter. Standardreferenz für Security Hub CSPM

Wenn Sie einen Standard aktivieren, aktiviert Security Hub CSPM automatisch alle Kontrollen, die für den Standard gelten. Security Hub CSPM führt dann Sicherheitsüberprüfungen an den Steuerelementen durch, wodurch Security Hub CSPM-Ergebnisse generiert werden. Sie können einzelne Steuerelemente bei Bedarf deaktivieren und später wieder aktivieren. Sie können einen Standard auch vollständig deaktivieren. Wenn Sie einen Standard deaktivieren, beendet Security Hub CSPM die Ausführung von Sicherheitsüberprüfungen für Kontrollen, die für den Standard gelten. Für die Kontrollen werden keine Ergebnisse mehr generiert.

Zusätzlich zu den Ergebnissen generiert Security Hub CSPM eine Sicherheitsbewertung für jeden Standard, den Sie aktivieren. Die Bewertung basiert auf dem Status der Kontrollen, die für den Standard gelten. Wenn Sie eine Aggregationsregion festlegen, spiegelt die Sicherheitsbewertung für einen Standard den Status der Kontrollen in allen verknüpften Regionen wider. Wenn Sie der Security Hub CSPM-Administrator einer Organisation sind, spiegelt die Bewertung den Status der Kontrollen für alle Konten in Ihrer Organisation wider. Weitere Informationen finden Sie unter Berechnung der Sicherheitswerte.

Um Standards zu überprüfen und zu verwalten, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Auf der Konsole werden auf der Seite Sicherheitsstandards alle Sicherheitsstandards angezeigt, die Security Hub CSPM derzeit unterstützt. Dies beinhaltet eine Beschreibung der einzelnen Standards und den aktuellen Status der Standards. Wenn Sie einen Standard aktivieren, können Sie auf dieser Seite auch auf zusätzliche Details zum Standard zugreifen. Sie können beispielsweise Folgendes überprüfen:

- Die aktuelle Sicherheitsbewertung für den Standard.
- Aggregierte Statistiken für Kontrollen, die für den Standard gelten.
- Eine Liste der Kontrollen, die für den Standard gelten und derzeit aktiviert sind, einschließlich des jeweiligen Konformitätsstatus.
- Eine Liste von Kontrollen, die für den Standard gelten, aber derzeit deaktiviert sind.

Für eine eingehendere Analyse können Sie die Daten filtern und sortieren und sich die Details der einzelnen Kontrollen ansehen, die für den Standard gelten.

Sie können Standards einzeln für ein einzelnes Konto aktivieren und AWS-Region. Um Zeit zu sparen und Konfigurationsabweichungen in Umgebungen mit mehreren Konten und mehreren Regionen zu

reduzieren, empfehlen wir jedoch, die Standards über eine zentrale Konfiguration zu aktivieren und zu verwalten. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Richtlinien erstellen, die festlegen, wie ein Standard für mehrere Konten und Regionen konfiguriert werden soll.

Themen

- Standardreferenz für Security Hub CSPM
- Einen Sicherheitsstandard aktivieren
- Überprüfung der Einzelheiten eines Sicherheitsstandards
- Beim Ausschalten automatisch aktivierter Sicherheitsstandards
- Deaktivierung eines Sicherheitsstandards

Standardreferenz für Security Hub CSPM

In AWS Security Hub CSPM besteht ein Sicherheitsstandard aus einer Reihe von Anforderungen, die auf regulatorischen Rahmenbedingungen, branchenüblichen Best Practices oder Unternehmensrichtlinien basieren. Security Hub CSPM ordnet diese Anforderungen den Kontrollen zu und führt Sicherheitsüberprüfungen der Kontrollen durch, um zu beurteilen, ob die Anforderungen eines Standards erfüllt werden. Jeder Standard umfasst mehrere Kontrollen.

Security Hub CSPM unterstützt derzeit die folgenden Standards:

- AWS Bewährte grundlegende Sicherheitsverfahren — Dieser Standard wurde von Branchenexperten entwickelt AWS und ist eine Zusammenstellung von bewährten Sicherheitsmethoden für Unternehmen, unabhängig von Branche oder Größe. Er bietet eine Reihe von Kontrollen, die erkennen, wenn Sie AWS-Konten und Ihre Ressourcen von den bewährten Sicherheitsmethoden abweichen. Es enthält auch präskriptive Anleitungen zur Verbesserung und Aufrechterhaltung Ihrer Sicherheitslage.
- Bewährte Methoden zur KI-Sicherheit — Dieser Standard wurde von AWS Sicherheitsexperten entwickelt und bietet eine Reihe kuratierter Kontrollen, mit denen erkannt wird, wenn die eingesetzten KI-Ressourcen nicht den bewährten Sicherheitsverfahren entsprechen. Es hilft Ihnen dabei, Bereiche zu identifizieren, in denen Ihre KI-Workloads von den empfohlenen Sicherheitskonfigurationen abweichen, und deckt Bereiche wie Netzwerkisolierung, Verschlüsselung, VPC-Platzierung und AWS KMS Schlüsselnutzung ab.
- AWS Resource Tagging — Mit diesem von Security Hub CSPM entwickelten Standard können Sie feststellen, ob Ihre AWS Ressourcen über Tags verfügen. Ein Tag ist ein Schlüssel-Wert-Paar,

das als Metadaten für eine Ressource fungiert. AWS Mithilfe von Tags können Sie Ressourcen identifizieren, kategorisieren, verwalten und nach ihnen suchen. AWS Sie können beispielsweise Tags verwenden, um Ressourcen nach Zweck, Eigentümer oder Umgebung zu kategorisieren.

- CIS AWS Foundations Benchmark — Dieser vom Center for Internet Security (CIS) entwickelte Standard bietet sichere Konfigurationsrichtlinien für AWS. Er legt eine Reihe von Richtlinien und bewährten Methoden zur Sicherheitskonfiguration für eine Untergruppe von AWS-Services Ressourcen fest, wobei der Schwerpunkt auf grundlegenden, testbaren und architekturunabhängigen Einstellungen liegt. Die Richtlinien beinhalten klare, schrittweise Implementierungs- und Bewertungsverfahren.
- NIST SP 800-53 Revision 5 — Dieser Standard entspricht den Anforderungen des National Institute of Standards and Technology (NIST) zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und kritischen Ressourcen. Der zugehörige Rahmen gilt im Allgemeinen für Bundesbehörden oder Organisationen, die mit Bundesbehörden oder Informationssystemen zusammenarbeiten U.S. U.S Private Organisationen können die Anforderungen jedoch auch als Richtschnur verwenden.
- NIST SP 800-171 Revision 2 — Dieser Standard entspricht den Sicherheitsempfehlungen und -anforderungen des NIST zum Schutz der Vertraulichkeit kontrollierter, nicht klassifizierter Informationen (CUI) in Systemen und Organisationen, die nicht Teil der Bundesregierung sind. U.S CUI sind Informationen, die nicht den behördlichen Klassifizierungskriterien entsprechen, aber als sensibel gelten und von der Bundesregierung oder anderen Stellen im Auftrag der Bundesregierung erstellt oder in Besitz genommen werden U.S. U.S
- PCI DSS — Dieser Standard entspricht dem vom PCI Security Standards Council (SSC) definierten Compliance-Framework für den Payment Card Industry Data Security Standard (PCI DSS). Das Framework enthält eine Reihe von Regeln und Richtlinien für den sicheren Umgang mit Kredit- und Debitkarteninformationen. Das Framework gilt im Allgemeinen für Organisationen, die Karteninhaberdaten speichern, verarbeiten oder übertragen.
- CRI Profile v2.2 — Dieser Standard entspricht dem CRI Profile, einem vom Cyber Risk Institute (CRI) entwickelten Compliance-Framework. Das Framework vereinheitlicht die Cybersicherheit und die regulatorischen Erwartungen, die für den Finanzdienstleistungssektor gelten, in einem gemeinsamen Anforderungskatalog. Der Rahmen gilt im Allgemeinen für Finanzinstitute und die Organisationen, die sie betreuen.
- Service-managed standard, AWS Control Tower — Dieser Standard hilft Ihnen bei der Konfiguration der von Security Hub CSPM bereitgestellten Detektivkontrollen von. AWS Control Tower AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten und dabei den vorgeschriebenen Best Practices zu folgen.

Die CSPM-Standards und -Kontrollen von Security Hub garantieren nicht die Einhaltung gesetzlicher Rahmenbedingungen oder Audits. Stattdessen bieten sie eine Möglichkeit, den Zustand Ihrer Ressourcen und Ihrer Ressourcen zu bewerten AWS-Konten und zu überwachen. Wir empfehlen, jeden Standard zu aktivieren, der für Ihre Geschäftsanforderungen, Ihre Branche oder Ihren Anwendungsfall relevant ist.

Einzelne Kontrollen können für mehr als einen Standard gelten. Wenn Sie mehrere Standards aktivieren, empfehlen wir, auch konsolidierte Kontrollergebnisse zu aktivieren. Wenn Sie dies tun, generiert Security Hub CSPM einen einzigen Befund für jedes Steuerelement, auch wenn das Steuerelement für mehr als einen Standard gilt. Wenn Sie konsolidierte Kontrollergebnisse nicht aktivieren, generiert Security Hub CSPM für jeden aktivierten Standard, für den eine Kontrolle gilt, einen separaten Befund. Wenn Sie beispielsweise zwei Standards aktivieren und eine Kontrolle für beide gilt, erhalten Sie zwei separate Ergebnisse für die Kontrolle, einen für jeden Standard. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis für die Kontrolle. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Detaillierte Referenz standardmäßig

- AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM
- Bewährte Methoden für KI-Sicherheit sind Standard im Security Hub CSPM
- AWS Standard für Ressourcen-Tagging in Security Hub CSPM
- CIS AWS Benchmark für Stiftungen im Security Hub CSPM
- NIST SP 800-53 Revision 5 im Security Hub CSPM
- NIST SP 800-171 Revision 2 im Security Hub CSPM
- PCI DSS im Security Hub CSPM
- CRI-Profil v2.2 im Security Hub CSPM
- Service-managed Standards im Security Hub CSPM

AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM

Der von AWS Branchenexperten entwickelte Standard AWS Foundational Security Best Practices (FSBP) ist eine Zusammenstellung von bewährten Sicherheitsmethoden für Unternehmen, unabhängig von Branche oder Größe. Er bietet eine Reihe von Kontrollen, die erkennen, wann AWS-Konten und welche Ressourcen von den bewährten Sicherheitsmethoden abweichen. Es

enthält auch präskriptive Leitlinien zur Verbesserung und Aufrechterhaltung der Sicherheitslage Ihres Unternehmens.

In AWS Security Hub CSPM umfasst der Standard AWS Foundational Security Best Practices Kontrollen, mit denen Sie AWS-Konten und Ihre Workloads kontinuierlich evaluieren und Ihnen helfen, Bereiche zu identifizieren, die von den bewährten Sicherheitsmethoden abweichen. Die Kontrollen beinhalten bewährte Sicherheitsverfahren für Ressourcen aus verschiedenen Quellen. AWS-Services Jedem Steuerelement wird eine Kategorie zugewiesen, die die Sicherheitsfunktion widerspiegelt, für die das Steuerelement gilt. Eine Liste der Kategorien und weitere Informationen finden Sie unterKategorien kontrollieren.

Kontrollen, die für den Standard gelten

In der folgenden Liste wird angegeben, welche AWS Security Hub CSPM-Steuerelemente für den Standard AWS Foundational Security Best Practices (v1.0.0) gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto

[ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

[APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

[APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

[APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert

[APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

[APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

[APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben

[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden

[APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden

[APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

[AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

[Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

[AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden

[BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden

[BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen

[BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden

[BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein

Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein

[CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

[CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden

[CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden

[CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

[CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer

[CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden

[Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen

[Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben

[Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein

[Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein

[Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

[DMS.9] DMS-Endpunkte sollten SSL verwenden

[DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben

[DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben

[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein

[DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

[DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Point-in-Time-Wiederherstellung aktiviert sein

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

[EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben

[EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

[EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

[EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

[EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren

[EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

[EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden

[EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden

[EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden

[EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden

[EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden

[EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein

[EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren

[EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

[EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination

[EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

[EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein

[EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

[ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

[ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

[ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

[ECS.12] ECS-Cluster sollten Container Insights verwenden

[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden

[ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben

[ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren

[ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren

[EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

[EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen

[EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein

[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

[EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein

[EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein

[ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein

[ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein

[ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

[ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

[ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

[ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein

[ELB.6] Bei Anwendung, Gateway und Network Load Balancers sollte der Löschschutz aktiviert sein

[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

[ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

[ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln

[ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden

[ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

[EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein

[EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden

[EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden

[ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

[ES.7] Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

[FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

[FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

[FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ

[FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ

[FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein

[Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden

[Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue

[GuardDuty.1] GuardDuty sollte aktiviert sein

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein

[GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein

[GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein

[GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein

[GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

[Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein

[Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein

[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein

[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

[Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

[KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

[Macie.1] Amazon Macie sollte aktiviert sein

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden

[MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein

[MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein

[MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

[Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

[Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

[NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein

Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein

[Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch

[Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein

[Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben

Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein

[PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein

[Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden

[RDS.1] Der RDS-Snapshot sollte privat sein

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

[RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

[RDS.11] Für RDS-Instances sollten automatische Backups aktiviert sein

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

[RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein

[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen

[RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden

[RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch

[RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern

[RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden

[RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein

[RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden

[RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden

[RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden

[RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein

[RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

[Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein

[RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

[RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein

[RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten

[RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden

[RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

[SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein

[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen

[SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

[SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein

Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein

[SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

[SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein

[SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

[SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden

[SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys

[SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation

[SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein

[SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein

[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

[SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch

[SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

[Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein

[WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein

[WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

[WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Bewährte Methoden für KI-Sicherheit sind Standard im Security Hub CSPM

Der Best Practices-Standard für KI Security besteht aus einer Reihe automatisierter Sicherheitsprüfungen, mit denen festgestellt wird, wenn die eingesetzten KI-Ressourcen nicht den bewährten Sicherheitsverfahren entsprechen. Dieser von AWS Sicherheitsexperten entwickelte Standard bietet eine kuratierte Reihe von Kontrollen, mit denen Sie Bereiche identifizieren können, in denen Ihre KI-Workloads von den empfohlenen Sicherheitskonfigurationen abweichen.

In AWS Security Hub CSPM umfasst der AI Security Best Practices-Standard Kontrollen, die Ihre Ressourcen kontinuierlich bewerten. Die Kontrollen decken Sicherheitsbereiche ab,

einschließlich, aber nicht beschränkt auf Netzwerkisolierung, Verschlüsselung im Ruhezustand und bei der Übertragung, VPC-Platzierung, AWS KMS Schlüsselnutzung und private Registrierungsanforderungen. Jedem Steuerelement wird eine Kategorie zugewiesen, die die Sicherheitsfunktion widerspiegelt, für die das Steuerelement gilt. Eine Liste der Kategorien und weitere Informationen finden Sie unterKontrollkategorien in Security Hub CSPM.

Der AI Security Best Practices-Standard hat den folgenden Amazon-Ressourcennamen (ARN):`arn:aws:securityhub:region::standards/ai-security-best-practices/v/1.0.0`, wobei der Regionalcode für die entsprechende *region* ist AWS-Region. Sie können auch den GetEnabledStandardsBetrieb der Security Hub CSPM-API verwenden, um den ARN eines Standards abzurufen, der derzeit aktiviert ist.

Kontrollen, die für den Standard gelten

In der folgenden Liste wird angegeben, welche AWS Security Hub CSPM-Steuerelemente für den AI Security Best Practices-Standard (v1.0.0) gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

- [Bedrock.1] Amazon Bedrock-Datenquellen sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- [BedrockAgentCore.7] Bedrock-Interpreter für AgentCore benutzerdefinierten Code sollten eine private Netzwerkkonfiguration verwenden
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SageMaker.20] Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.21] SageMaker Notebook-Instances sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [SageMaker.22] In den SageMaker Überwachungsplänen sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.23] Bei SageMaker Inferenzexperimenten sollte das Instanz-Speichervolumen verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [SageMaker.24] Bei SageMaker Inferenzexperimenten sollte der Datenspeicher verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [SageMaker.25] Bei Jobdefinitionen in SageMaker Modellqualität sollte die Netzwerkisolierung aktiviert sein

AWS Standard für Ressourcen-Tagging in Security Hub CSPM

Mit dem AWS Resource Tagging-Standard, der von AWS Security Hub CSPM entwickelt wurde, können Sie feststellen, ob in Ihren AWS Ressourcen Tags fehlen. Tags sind Schlüssel-Wert-Paare, die als Metadaten für die Organisation von Ressourcen dienen. AWS Bei den meisten AWS Ressourcen haben Sie die Möglichkeit, einer Ressource Tags hinzuzufügen, wenn Sie die Ressource erstellen oder nachdem Sie die Ressource erstellt haben. Zu den Ressourcen gehören beispielsweise CloudFront Amazon-Distributionen, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Secrets in. AWS Secrets Manager Mithilfe von Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern AWS .

Jedes -Tag besteht aus zwei Teilen:

- Ein Tag-Schlüssel, zum Beispiel, `CostCenter` `Environment`, oder. `Project` Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Ein Tag-Wert, zum Beispiel oder. `111122223333` `Production` Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Informationen zum Hinzufügen von Tags zu AWS Ressourcen finden Sie im Benutzerhandbuch zum Kennzeichnen von AWS Ressourcen und zum Tag-Editor.

Für jedes Steuerelement, das für den AWS Resource Tagging-Standard in Security Hub CSPM gilt, können Sie optional den unterstützten Parameter verwenden, um Tag-Schlüssel anzugeben, nach denen das Steuerelement suchen soll. Wenn Sie keine Tag-Schlüssel angeben, prüft das Steuerelement nur, ob mindestens ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn eine Ressource keine Tag-Schlüssel hat.

Bevor Sie den AWS Resource Tagging-Standard aktivieren, ist es wichtig, die Ressourcenaufzeichnung in AWS Config zu aktivieren und zu konfigurieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten. Weitere Informationen, einschließlich einer Liste der aufzuzeichnenden Ressourcentypen, finden Sie unter. Erforderliche AWS Config Ressourcen für Kontrollbefunde

Nachdem Sie den AWS Resource Tagging-Standard aktiviert haben, erhalten Sie erste Ergebnisse für Kontrollen, die für diesen Standard gelten. Beachten Sie, dass es bis zu 18 Stunden dauern kann, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie Kontrollen, die für andere aktivierte Standards gelten. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Der AWS Resource Tagging-Standard hat den folgenden Amazon-Ressourcennamen (ARN):`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`, wobei der Regionalcode für die entsprechende *`region`* AWS-Region ist. Sie können auch den GetEnabledStandardsBetrieb der Security Hub CSPM-API verwenden, um den ARN eines Standards abzurufen, der derzeit aktiviert ist.

> **Note**
>
> Der AWS Resource Tagging-Standard ist in den Regionen Asien-Pazifik (Neuseeland) und Asien-Pazifik (Taipeh) nicht verfügbar.

Kontrollen, die für den Standard gelten

Die folgende Liste gibt an, welche AWS Security Hub CSPM-Steuerelemente für den AWS Resource Tagging-Standard (v1.0.0) gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden

- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten mit Tags versehen werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Backup.5] AWS Backup Backup-Pläne sollten mit einem Tag versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [CloudFormation.2] CloudFormation Stacks sollten markiert werden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden

- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DynamoDB.5] DynamoDB-Tabellen sollten markiert werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten mit Tags versehen werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten mit Tags versehen werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.13] ECS-Services sollten markiert werden
- [ECS.14] ECS-Cluster sollten markiert werden

- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten markiert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.23] IAM Access Analyzer-Analyzer sollten gekennzeichnet sein
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden

- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] Snapshots von RDS-DB-Clustern sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden

- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden
- [Transfer.1] AWS Transfer Family Workflows sollten mit Tags versehen werden
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden

CIS AWS Benchmark für Stiftungen im Security Hub CSPM

Der Center for Internet Security (CIS) AWS Foundations Benchmark dient als eine Reihe von bewährten Methoden zur Sicherheitskonfiguration für AWS. Diese branchenweit anerkannten Best Practices bieten Ihnen klare, schrittweise Implementierungs- und Bewertungsverfahren. Die Kontrollen in diesem Benchmark reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und helfen Ihnen dabei, die spezifischen Systeme zu schützen, die Ihr Unternehmen verwendet.

AWS Security Hub CSPM unterstützt die CIS AWS Foundations Benchmark-Versionen 5.0.0, 3.0.0, 1.4.0 und 1.2.0. Auf dieser Seite sind die Sicherheitskontrollen aufgeführt, die jede Version unterstützt. Sie bietet auch einen Vergleich der Versionen.

CIS AWS Foundations Benchmark Version 5.0.0

Security Hub CSPM unterstützt Version 5.0.0 (v5.0.0) des CIS Foundations Benchmark. AWS Security Hub CSPM hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark für CIS AWS Foundations Benchmark, v5.0.0, Stufe 1
- CIS-Benchmark für CIS AWS Foundations Benchmark, v5.0.0, Stufe 2

Kontrollen, die für die CIS gelten AWS Benchmark für Stiftungen, Version 5.0.0

[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen

[EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS

[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

[IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

[S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

CIS AWS Benchmark für Stiftungen, Version 3.0.0

Security Hub CSPM unterstützt Version 3.0.0 (v3.0.0) des CIS Foundations Benchmark. AWS Security Hub CSPM hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS-Benchmark für CIS AWS Foundations Benchmark, v3.0.0, Stufe 1
- CIS-Benchmark für CIS AWS Foundations Benchmark, v3.0.0, Stufe 2

Kontrollen, die für die CIS gelten AWS Benchmark für Stiftungen, Version 3.0.0

[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen

[EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

[IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

[S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

CIS AWS Benchmark für Stiftungen Version 1.4.0

Security Hub CSPM unterstützt Version 1.4.0 (v1.4.0) des CIS Foundations Benchmark. AWS

Kontrollen, die für die CIS gelten AWS Benchmark für Stiftungen, Version 1.4.0

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

CIS AWS Benchmark für Stiftungen Version 1.2.0

Security Hub CSPM unterstützt Version 1.2.0 (v1.2.0) des CIS Foundations Benchmark. AWS Security Hub CSPM hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark für CIS AWS Foundations Benchmark, v1.2.0, Stufe 1
- CIS Benchmark für CIS AWS Foundations Benchmark, v1.2.0, Stufe 2

Kontrollen, die für die CIS gelten AWS Benchmark für Stiftungen Version 1.2.0

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein

[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

[CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22

[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

[IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

Versionsvergleich für CIS AWS Maßstab für Stiftungen

In diesem Abschnitt werden die Unterschiede zwischen bestimmten Versionen des Center for Internet Security (CIS) AWS Foundations Benchmark — v5.0.0, v3.0.0, v1.4.0 und v1.2.0 — zusammengefasst. AWS Security Hub CSPM unterstützt jede dieser Versionen des CIS AWS Foundations Benchmark. Wir empfehlen jedoch, Version 5.0.0 zu verwenden, um über bewährte Sicherheitsmethoden auf dem Laufenden zu bleiben. Sie können mehrere Versionen der Benchmark-Standards von CIS AWS Foundations gleichzeitig aktivieren. Informationen zur Aktivierung von Standards finden Sie unterEinen Sicherheitsstandard aktivieren. Wenn Sie auf v5.0.0 aktualisieren möchten, aktivieren Sie es, bevor Sie eine ältere Version deaktivieren. Dadurch werden Lücken in Ihren Sicherheitsüberprüfungen vermieden. Wenn Sie die Security Hub CSPM-Integration mit verwenden AWS Organizations und v5.0.0 in mehreren Konten stapelweise aktivieren möchten, empfehlen wir die zentrale Konfiguration.

Zuordnung der Kontrollen zu den CIS-Anforderungen in jeder Version

Verstehen Sie, welche Kontrollen jede Version des CIS AWS Foundations Benchmark unterstützt.

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto	1.2	1.2	1.2	1.18
[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben	3.5	3.5	3.7	2.7
[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein	3.2	3.2	3.2	2.2
[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.4	2.4
[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.3	2.3

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	3.4	3.4	3.6	2.6
[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.3	3.3
[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.1
[CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.2
[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.4	3.4

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.5	3.5
[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.6	3.6
[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.7	3.7
[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.8	3.8
[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4,9 bis 4,9	3.9

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.10	3,10
[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.11	3,11
[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.12	3,12
[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.13	3.13
[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	4.14	3,14
[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden	3.3	3.3	3.5	2.5

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	5.5	5.4	5.3	4.3
[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein	3.7	3.7	3.9	2,9
[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein	5.1.1	2.2.1	2.2.1	Nicht unterstützt
[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden	5,7	5.6	Nicht unterstützt	Nicht unterstützt
[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22	Nicht unterstützt — ersetzt durch die Anforderungen 5.3 und 5.4	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.1
[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389	Nicht unterstützt — ersetzt durch die Anforderungen 5.3 und 5.4	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.2

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389	5.2	5.1	5.1	Nicht unterstützt
[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers	5.3	5.2	Nicht unterstützt	Nicht unterstützt
[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen	5.4	5.3	Nicht unterstützt	Nicht unterstützt
[EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS	2.3.1	2.4.1	Nicht unterstützt	Nicht unterstützt
[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden	2.3.1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	Nicht unterstützt	Nicht unterstützt	1.16	1,22
[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein	1.14	1.15	Nicht unterstützt	1.16

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	1.13	1.14	1.14	1.4
[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	1.3	1.4	1.4	1.12
[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben	1.9	1.10	1.10	1.2
[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein	1.5	1,6	1,6	1.14
[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	Nicht unterstützt — siehe stattdessen [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	Nicht unterstützt — siehe [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden stattdessen	Nicht unterstützt — siehe [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden stattdessen	1.3

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	1.4	1.5	1.5	1.13
[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.5
[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,6
[IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,7
[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.8
[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	1,7	1.8	1.8	1.9

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern	1.8	1.9	1.9	1.10
[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.11
[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support	1.16	1,17	1,17	1.2
[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.1
[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	1.11	1.12	1.12	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	1.18	1,19	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess	1.21	1,22	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein	1.19	1,20	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein	3.6	3.6	3.8	2.8
[Macie.1] Amazon Macie sollte aktiviert sein	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten	2.2.3	2.3.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein	2.2.1	2.3.1	2.3.1	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden	2.2.4	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein	2.2.2	2.3.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden	2.2.4	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	2.1.4	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein	2.1.1	2.1.1	2.1.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	2.1.4	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

Kontroll-ID und Titel	CIS v5.0.0-Anforderung	CIS v3.0.0-Anforderung	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	2.1.2	2.1.2	2.1.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

ARNs für die CIS AWS Benchmarks für Stiftungen

Wenn Sie eine oder mehrere Versionen des CIS AWS Foundations Benchmark aktivieren, erhalten Sie ab sofort Ergebnisse im AWS Security Finding Format (ASFF). In ASFF verwendet jede Version den folgenden Amazon-Ressourcennamen (ARN):

Benchmark AWS v5.0.0 für CIS Foundations

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/5.0.0
```

Benchmark AWS v3.0.0 für CIS Foundations

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Benchmark AWS v1.4.0 für CIS Foundations

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Benchmark AWS v1.2.0 für CIS Foundations

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Sie können den GetEnabledStandardsBetrieb der Security Hub CSPM-API verwenden, um den ARN eines aktivierten Standards zu ermitteln.

Die vorherigen Werte sind für. `StandardsArn` `StandardsSubscriptionArn`Bezieht sich jedoch auf die Standard-Abonnementressource, die Security Hub CSPM erstellt, wenn Sie einen Standard abonnieren, indem Sie BatchEnableStandardsin einer Region anrufen.

> **Note**
>
> Wenn Sie eine Version des CIS AWS Foundations Benchmark aktivieren, kann es bis zu 18 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie aktivierte Kontrollen in anderen aktivierten Standards. Weitere Informationen zum Zeitplan für die Generierung von Kontrollbefunden finden Sie unter. Zeitplan für die Ausführung von Sicherheitsprüfungen

Suchfelder unterscheiden sich, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Informationen zu diesen Unterschieden finden Sie unterAuswirkungen der Konsolidierung auf ASFF-Felder und -Werte. Ergebnisse der Stichprobenkontrolle finden Sie unterStichproben von Kontrollbefunden.

CIS-Anforderungen, die in Security Hub CSPM nicht unterstützt werden

Wie in der obigen Tabelle angegeben, unterstützt Security Hub CSPM nicht jede CIS-Anforderung in jeder Version des CIS AWS Foundations Benchmark. Viele der nicht unterstützten Anforderungen können nur bewertet werden, indem der Status Ihrer Ressourcen manuell überprüft wird. AWS

NIST SP 800-53 Revision 5 im Security Hub CSPM

Die NIST-Sonderveröffentlichung 800-53 Revision 5 (NIST SP 800-53 Rev. 5) ist ein Framework für Cybersicherheit und Compliance, das vom National Institute of Standards and Technology (NIST) entwickelt wurde, einer Behörde, die Teil des ist. U.S Handelsministerium. Dieses Compliance-Framework enthält einen Katalog von Sicherheits- und Datenschutzanforderungen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und kritischen Ressourcen. U.S. Bundesbehörden und Auftragnehmer müssen diese Anforderungen erfüllen, um ihre Systeme und Organisationen zu schützen. Private Organisationen können die Anforderungen auch freiwillig als Leitfaden für die Reduzierung des Cybersicherheitsrisikos verwenden. Weitere Informationen über das Framework und seine Anforderungen finden Sie unter NIST SP 800-53 Rev. 5 im NIST Computer Security Resource Center.

AWS Security Hub CSPM bietet Sicherheitskontrollen, die einen Teil der Anforderungen von NIST SP 800-53 Revision 5 unterstützen. Die Kontrollen führen automatisierte Sicherheitsprüfungen für bestimmte Ressourcen durch. AWS-Services Um diese Kontrollen zu aktivieren und zu verwalten,

können Sie das NIST SP 800-53 Revision 5-Framework standardmäßig in Security Hub CSPM aktivieren. Beachten Sie, dass die Steuerungen die Anforderungen von NIST SP 800-53 Revision 5, die manuelle Prüfungen erfordern, nicht unterstützen.

Im Gegensatz zu anderen Frameworks schreibt das NIST SP 800-53 Revision 5-Framework nicht vor, wie seine Anforderungen bewertet werden sollten. Stattdessen enthält das Framework Richtlinien. In Security Hub CSPM stellen der Standard und die Kontrollen von NIST SP 800-53 Revision 5 das Verständnis des Dienstes in Bezug auf diese Richtlinien dar.

Themen

- Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten
- Feststellen, welche Kontrollen für den Standard gelten

Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten

Um die Abdeckung und die Genauigkeit der Ergebnisse zu optimieren, ist es wichtig, die Ressourcenaufzeichnung zu aktivieren und zu konfigurieren, AWS Config bevor Sie den Standard NIST SP 800-53 Revision 5 in AWS Security Hub CSPM aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Dies gilt in erster Linie für Steuerelemente mit einem Zeitplantyp, der durch Änderung ausgelöst wurde. Für einige Steuerelemente mit einem periodischen Zeitplan ist jedoch auch die Erfassung von Ressourcen erforderlich. Wenn die Ressourcenaufzeichnung nicht aktiviert oder korrekt konfiguriert ist, ist Security Hub CSPM möglicherweise nicht in der Lage, die entsprechenden Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten.

Informationen darüber, wie Security Hub CSPM die Ressourcenaufzeichnung in verwendet AWS Config, finden Sie unter. Aktivierung und Konfiguration AWS Config für Security Hub CSPM Informationen zur Konfiguration der Ressourcenaufzeichnung in AWS Config finden Sie unter Arbeiten mit dem Konfigurationsrekorder im AWS Config Entwicklerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen aufgeführt, die für Kontrollen aufgezeichnet werden müssen, die für den Standard NIST SP 800-53 Revision 5 in Security Hub CSPM gelten.

AWS-Service	Ressourcentypen
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

AWS-Service	Ressourcentypen
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Grundgestein AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`

AWS-Service	Ressourcentypen
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

AWS-Service	Ressourcentypen
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

AWS-Service	Ressourcentypen
Amazon SageMaker KI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Feststellen, welche Kontrollen für den Standard gelten

In der folgenden Liste sind die Kontrollen aufgeführt, die die Anforderungen von NIST SP 800-53 Revision 5 unterstützen und für den Standard NIST SP 800-53 Revision 5 in AWS Security Hub CSPM gelten. Einzelheiten zu den spezifischen Anforderungen, die ein Steuerelement unterstützt, erhalten Sie, wenn Sie das Steuerelement auswählen. Weitere Informationen finden Sie in den Details für das Steuerelement im Feld „Verwandte Anforderungen“. Dieses Feld gibt jede NIST-Anforderung an, die das Steuerelement unterstützt. Wenn das Feld keine bestimmte NIST-Anforderung spezifiziert, unterstützt das Steuerelement die Anforderung nicht.

- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert

- [APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
- [CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
- [CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
- [CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Point-in-Time-Wiederherstellung aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind
- [EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden
- [EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
- [EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden

- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden
- [ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein
- [ELB.6] Bei Anwendung, Gateway und Network Load Balancers sollte der Löschschutz aktiviert sein
- [ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein
- [ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben
- [ES.7] Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden
- [ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein

- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.11] Für RDS-Instances sollten automatische Backups aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren
- [RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden
- [RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden
- [RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden
- [RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden
- [RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren
- [S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
- [S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.1] SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein

NIST SP 800-171 Revision 2 im Security Hub CSPM

Die NIST-Sonderveröffentlichung 800-171 Revision 2 (NIST SP 800-171 Rev. 2) ist ein Framework für Cybersicherheit und Compliance, das vom National Institute of Standards and Technology (NIST) entwickelt wurde, einer Behörde, die Teil des ist. U.S Handelsministerium. Dieses Compliance-Framework enthält empfohlene Sicherheitsanforderungen für den Schutz der Vertraulichkeit kontrollierter, nicht klassifizierter Informationen in Systemen und Organisationen, die nicht Teil der

Bundesregierung sind U.S. Kontrollierte, nicht klassifizierte Informationen, auch CUI genannt, sind vertrauliche Informationen, die nicht den behördlichen Klassifizierungskriterien entsprechen, aber geschützt werden müssen. Es handelt sich um Informationen, die als sensibel gelten und von der U.S Bundesregierung oder anderen Stellen im Auftrag der Bundesregierung erstellt wurden oder in deren Besitz sind U.S.

NIST SP 800-171 Rev. 2 enthält empfohlene Sicherheitsanforderungen zum Schutz der Vertraulichkeit von CUI in folgenden Fällen:

- Die Informationen befinden sich in nichtföderalen Systemen und Organisationen,
- Die nichtföderale Organisation sammelt oder verwaltet keine Informationen im Auftrag einer Bundesbehörde und nutzt oder betreibt kein System im Auftrag einer Behörde, und
- Für die CUI-Kategorie, die im CUI-Register aufgeführt ist, gibt es keine spezifischen Schutzanforderungen zum Schutz der Vertraulichkeit von CUI, die in den Genehmigungsgesetzen, Verordnungen oder behördlichen Richtlinien vorgeschrieben sind.

Die Anforderungen gelten für alle Komponenten nichtstaatlicher Systeme und Organisationen, die CUI verarbeiten, speichern oder übertragen oder die Komponenten schützen. Weitere Informationen finden Sie unter NIST SP 800-171 Rev. 2 im NIST Computer Security Resource Center.

AWS Security Hub CSPM bietet Sicherheitskontrollen, die einen Teil der Anforderungen von NIST SP 800-171 Revision 2 unterstützen. Die Kontrollen führen automatisierte Sicherheitsprüfungen für bestimmte Ressourcen durch. AWS-Services Um diese Kontrollen zu aktivieren und zu verwalten, können Sie das NIST SP 800-171 Revision 2-Framework standardmäßig in Security Hub CSPM aktivieren. Beachten Sie, dass die Steuerungen die Anforderungen von NIST SP 800-171 Revision 2, die manuelle Prüfungen erfordern, nicht unterstützen.

Themen

- Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten
- Festlegung, welche Kontrollen für den Standard gelten

Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten

Um die Abdeckung und die Genauigkeit der Ergebnisse zu optimieren, ist es wichtig, die Ressourcenaufzeichnung zu aktivieren und zu konfigurieren, AWS Config bevor Sie den Standard NIST SP 800-171 Revision 2 in AWS Security Hub CSPM aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch

die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten.

Informationen darüber, wie Security Hub CSPM die Ressourcenaufzeichnung in verwendet AWS Config, finden Sie unter. Aktivierung und Konfiguration AWS Config für Security Hub CSPM Informationen zur Konfiguration der Ressourcenaufzeichnung in AWS Config finden Sie unter Arbeiten mit dem Konfigurationsrekorder im AWS Config Entwicklerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen aufgeführt, die für Kontrollen aufgezeichnet werden müssen, die für den Standard NIST SP 800-171 Revision 2 in Security Hub CSPM gelten.

AWS-Service	Ressourcentypen
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(ICH BIN)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

AWS-Service	Ressourcentypen
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Festlegung, welche Kontrollen für den Standard gelten

In der folgenden Liste sind die Kontrollen aufgeführt, die die Anforderungen von NIST SP 800-171 Revision 2 unterstützen und für den Standard NIST SP 800-171 Revision 2 in AWS Security Hub CSPM gelten. Einzelheiten zu den spezifischen Anforderungen, die ein Steuerelement unterstützt, erhalten Sie, wenn Sie das Steuerelement auswählen. Weitere Informationen finden Sie in den Details für das Steuerelement im Feld „Verwandte Anforderungen“. Dieses Feld gibt jede NIST-Anforderung an, die das Steuerelement unterstützt. Wenn das Feld keine bestimmte NIST-Anforderung spezifiziert, unterstützt das Steuerelement die Anforderung nicht.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
- [CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein
- [CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
- [CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
- [CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
- [CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

- [CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind
- [CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung
- [CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
- [CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind
- [CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration
- [CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
- [CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
- [CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
- [CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
- [CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
- Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden
- [EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen

- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [SNS.1] SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein

PCI DSS im Security Hub CSPM

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Compliance-Framework eines Drittanbieters, das eine Reihe von Regeln und Richtlinien für den sicheren Umgang mit Kredit- und Debitkarteninformationen enthält. Der PCI Security Standards Council (SSC) erstellt und aktualisiert dieses Framework.

AWS Security Hub CSPM bietet einen PCI-DSS-Standard, der Ihnen helfen kann, die Einhaltung dieses Drittanbieter-Frameworks zu gewährleisten. Sie können diesen Standard verwenden, um Sicherheitslücken in AWS Ressourcen zu entdecken, die Karteninhaberdaten verarbeiten. Wir empfehlen, diesen Standard zu aktivieren AWS-Konten , wenn Ressourcen zur Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten oder sensiblen Authentifizierungsdaten vorhanden sind. Durch Prüfungen durch das PCI SSC wurde dieser Standard bestätigt.

Security Hub CSPM bietet Unterstützung für PCI DSS v3.2.1 und PCI DSS v4.0.1. Wir empfehlen die Verwendung von Version 4.0.1, um über bewährte Sicherheitsmethoden auf dem Laufenden zu bleiben. Sie können beide Versionen des Standards gleichzeitig aktivieren. Informationen zur Aktivierung von Standards finden Sie unterEinen Sicherheitsstandard aktivieren. Wenn Sie derzeit Version 3.2.1 verwenden, aber nur Version 4.0.1 verwenden möchten, aktivieren Sie die neuere Version, bevor Sie die ältere Version deaktivieren. Dadurch werden Lücken in Ihren Sicherheitsüberprüfungen vermieden. Wenn Sie die Security Hub CSPM-Integration mit verwenden AWS Organizations und v4.0.1 in mehreren Konten stapelweise aktivieren möchten, empfehlen wir, dafür die zentrale Konfiguration zu verwenden.

In den folgenden Abschnitten wird angegeben, welche Kontrollen für PCI DSS v3.2.1 und PCI DSS v4.0.1 gelten.

Kontrollen, die für PCI DSS v3.2.1 gelten

Die folgende Liste gibt an, welche Security Hub CSPM-Steuerelemente für PCI DSS v3.2.1 gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden

[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

[ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[GuardDuty.1] GuardDuty sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein

[Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein

[RDS.1] Der RDS-Snapshot sollte privat sein

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

Kontrollen, die für PCI DSS v4.0.1 gelten

Die folgende Liste gibt an, welche Security Hub CSPM-Steuerelemente für PCI DSS v4.0.1 gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

[ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben

[DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben

[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

[DMS.9] DMS-Endpunkte sollten SSL verwenden

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22

[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

[EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

[ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

[EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

[EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein

[ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein

[ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

[ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

[ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

[EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

[GuardDuty.1] GuardDuty sollte aktiviert sein

[GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

[GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

[IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

[Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein

[Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein

[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein

[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein

Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein

[Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein

[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

[Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

[S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

[WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein

[WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein

CRI-Profil v2.2 im Security Hub CSPM

Das CRI-Profil ist ein Cybersicherheits-Framework, das vom Cyber Risk Institute (CRI), einer gemeinnützigen Koalition von Finanzinstituten und Handelsverbänden, entwickelt wurde. Das Framework vereinheitlicht die Cybersicherheit und die regulatorischen Erwartungen an den Finanzdienstleistungssektor in einem gemeinsamen Anforderungskatalog. Auf diese Weise kann sich ein Unternehmen einmal selbst bewerten und dann anhand mehrerer Vorschriften Bericht erstatten. Weitere Informationen zum Framework und seinen Anforderungen finden Sie in der CRI-Profilübersicht auf der Website des Cyber Risk Institute.

AWS Security Hub CSPM bietet Sicherheitskontrollen, die einen Teil der Anforderungen von CRI Profile v2.2 unterstützen. Die Kontrollen führen automatisierte Sicherheitsprüfungen für bestimmte

Ressourcen durch. AWS-Services Um diese Kontrollen zu aktivieren und zu verwalten, können Sie CRI Profile v2.2 standardmäßig in Security Hub CSPM aktivieren. Beachten Sie, dass die Steuerelemente die Anforderungen von CRI Profile v2.2 nicht unterstützen, die manuelle Prüfungen erfordern.

Die Aktivierung dieses Standards und das Bestehen der Prüfungen für seine Kontrollen allein stellen noch keine Bestätigung der Einhaltung von CRI Profile v2.2 dar. Die Einhaltung der Vorschriften hängt von organisatorischen und betrieblichen Praktiken ab, die Security Hub CSPM nicht bewerten kann.

Themen

- Kontrollen, die für den Standard gelten

Kontrollen, die für den Standard gelten

In der folgenden Liste wird angegeben, welche Security Hub CSPM-Steuerelemente für CRI Profile v2.2 gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert
- [APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben

- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
- [CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
- [CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein
- [CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
- [CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
- [CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
- [CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind
- [CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
- [CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind
- [CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung
- [CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

- [CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind
- [CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration
- [CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
- [CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
- [CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
- [CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
- [CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
- Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Point-in-Time-Wiederherstellung aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind
- [EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden
- [EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
- [EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren

- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden
- [ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein
- [ELB.6] Bei Anwendung, Gateway und Network Load Balancers sollte der Löschschutz aktiviert sein
- [ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein

- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein
- [ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben
- [ES.7] Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden
- [ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein

- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein

- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.11] Für RDS-Instances sollten automatische Backups aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren
- [RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden
- [RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden
- [RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden
- [RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden
- [RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren
- [S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
- [S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.1] SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen

- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Service-managed Standards im Security Hub CSPM

Ein vom Service verwalteter Standard ist ein Sicherheitsstandard, der von einem anderen AWS-Service verwaltet wird, den Sie jedoch in Security Hub CSPM einsehen können. Zum Beispiel ist Service-Managed Standard: ein vom Service verwalteter Standard, der verwaltet AWS Control Tower wird. AWS Control Tower Ein Service-Managed-Standard unterscheidet sich auf folgende Weise von einem AWS Sicherheitsstandard, den Security Hub CSPM verwaltet:

- Erstellung und Löschung von Standards — Sie erstellen und löschen einen vom Service verwalteten Standard mit der Konsole oder API des verwaltenden Dienstes oder mit dem. AWS CLI Solange Sie den Standard nicht auf eine dieser Arten im Verwaltungsdienst erstellt haben, wird der Standard nicht in der Security Hub CSPM-Konsole angezeigt und ist nicht über die Security Hub CSPM-API zugänglich oder. AWS CLI
- Keine automatische Aktivierung von Kontrollen — Wenn Sie einen vom Service verwalteten Standard erstellen, aktivieren Security Hub CSPM und der Verwaltungsdienst nicht automatisch die Kontrollen, die für den Standard gelten. Wenn Security Hub CSPM neue Kontrollen für den Standard veröffentlicht, werden diese außerdem nicht automatisch aktiviert. Dies ist eine Abkehr von den Standards, die Security Hub CSPM verwaltet. Weitere Informationen zur üblichen Konfiguration von Steuerelementen in Security Hub CSPM finden Sie unter. Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM
- Steuerungen aktivieren und deaktivieren — Wir empfehlen, die Steuerungen im Verwaltungsdienst zu aktivieren und zu deaktivieren, um Abweichungen zu vermeiden.
- Verfügbarkeit von Kontrollen — Der Verwaltungsdienst entscheidet, welche Kontrollen im Rahmen des vom Service verwalteten Standards verfügbar sind. Die verfügbaren Kontrollen können alle oder einen Teil der vorhandenen Security Hub CSPM-Steuerelemente umfassen.

Nachdem der Verwaltungsdienst den vom Service verwalteten Standard erstellt und Kontrollen dafür verfügbar gemacht hat, können Sie in der Security Hub CSPM-Konsole, der Security Hub CSPM-API oder auf Ihre Kontrollergebnisse, Kontrollstatus und Standardsicherheitsbewertung zugreifen. AWS CLI Einige oder alle dieser Informationen sind möglicherweise auch im Verwaltungsdienst verfügbar.

Wählen Sie einen vom Service verwalteten Standard aus der folgenden Liste aus, um weitere Informationen zu diesem Standard zu erhalten.

Service-managed Standards

- Service-Managed Norm: AWS Control Tower

Service-Managed Norm: AWS Control Tower

Dieser Abschnitt enthält Informationen zu Service-Managed Standard:. AWS Control Tower

Was ist Service-Managed Standard: AWS Control Tower?

Service-Managed Standard: AWS Control Tower ist ein vom Service verwalteter Standard, der eine Teilmenge der Security Hub-Steuerelemente AWS Control Tower verwaltet und unterstützt. Dieser Standard richtet sich an Benutzer von AWS Security Hub CSPM und. AWS Control Tower Damit können Sie die Detective Controls von Security Hub CSPM vom AWS Control Tower Service aus konfigurieren.

Detective Controls erkennt die Nichtkonformität von Ressourcen (z. B. Fehlkonfigurationen) in Ihrem. AWS-Konten

> **Tip**
>
> Service-managed Standards unterscheiden sich von den Standards, die AWS Security Hub CSPM verwaltet. Beispielsweise müssen Sie im Verwaltungsdienst einen vom Dienst verwalteten Standard erstellen und löschen. Weitere Informationen finden Sie unter Service-managed Standards im Security Hub CSPM.

Wenn Sie eine Security Hub-CSPM-Steuerung aktivieren AWS Control Tower, aktiviert Control Tower auch Security Hub CSPM für Sie in diesen spezifischen Konten und Regionen, sofern dies nicht bereits aktiviert ist. In der Security Hub CSPM-Konsole und API können Sie Service-Managed Standard: AWS Control Tower zusammen mit anderen Security Hub CSPM-Standards anzeigen, sobald der Standard aktiviert ist. AWS Control Tower

Weitere Informationen zu diesem Standard finden Sie unter Security Hub CSPM-Steuerelemente im AWS Control Tower Benutzerhandbuch.

Den Standard erstellen

Dieser Standard ist in Security Hub CSPM nur verfügbar, wenn Sie Security Hub CSPM-Steuerungen von aktivieren. AWS Control Tower AWS Control Tower erstellt den Standard, wenn Sie ein entsprechendes Steuerelement zum ersten Mal mithilfe einer der folgenden Methoden aktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die `EnableControl`API auf)
- AWS CLI (führe den `enable-control`Befehl aus)

Wenn Sie eine Security Hub CSPM-Steuerung aktivieren, aktiviert Security Hub CSPM AWS Control Tower, sofern Sie Security Hub CSPM noch nicht aktiviert haben, AWS Control Tower auch Security Hub CSPM für Sie in diesen spezifischen Konten und Regionen.

Um ein Security Hub-CSPM-Steuerelement anhand der Kontroll-ID im Kontrollkatalog zu identifizieren, können Sie das Feld `Implementation.Identifier` in verwenden. AWS Control Tower Dieses Feld ist der Security Hub CSPM-Steuer-ID zugeordnet und kann verwendet werden, um nach einer bestimmten Kontroll-ID zu filtern. Um Kontrollmetadaten für ein bestimmtes Security Hub CSPM-Steuerelement (z. B. "CodeBuild.1„) in abzurufen AWS Control Tower, können Sie die `ListControls`API verwenden:

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Sie können diesen Standard nicht in der Security Hub CSPM-Konsole, der Security Hub CSPM-API oder AWS CLI ohne vorherige Einrichtung AWS Control Tower und Aktivierung der Security Hub CSPM-Steuerelemente AWS Control Tower mit einer der oben genannten Methoden anzeigen oder darauf zugreifen.

Dieser Standard ist nur dort verfügbar, wo er verfügbar ist.AWS-RegionenAWS Control Tower

Steuerungen im Standard aktivieren und deaktivieren

Nachdem Sie Security Hub CSPM Controls aktiviert haben AWS Control Tower und der Service-Managed Standard: AWS Control Tower Standard erstellt wurde, können Sie den Standard und die verfügbaren Kontrollen in Security Hub CSPM einsehen.

Wenn Security Hub CSPM dem Service-Managed Standard: AWS Control Tower Standard neue Kontrollen hinzufügt, werden diese nicht automatisch für Kunden aktiviert, die den Standard aktiviert haben. Sie sollten die Kontrollen für den Standard AWS Control Tower von mit einer der folgenden Methoden aktivieren und deaktivieren:

- AWS Control Tower Konsole

- AWS Control Tower API (rufen Sie die `DisableControl`APIs `EnableControl`und auf)
- AWS CLI (führe die `disable-control`Befehle `enable-control`und aus)

Wenn Sie den Aktivierungsstatus eines Steuerelements in ändern AWS Control Tower, spiegelt sich die Änderung auch in Security Hub CSPM wider.

Die Deaktivierung eines Steuerelements in Security Hub CSPM, das aktiviert ist, AWS Control Tower führt jedoch zu Kontrollabweichungen. Der Kontrollstatus in AWS Control Tower wird als angezeigt. `Drifted` Sie können diese Abweichung beheben, indem Sie die ResetEnabledControlAPI verwenden, um die Steuerung zurückzusetzen, bei der Drift aktiv ist, oder indem Re-register Sie in der AWS Control Tower Konsole OU auswählen oder indem Sie die Steuerung deaktivieren und erneut aktivieren, indem AWS Control Tower Sie eine der oben genannten Methoden verwenden.

Wenn Sie die Aktivierungs- und Deaktivierungsaktionen in AWS Control Tower abschließen, können Sie Kontrollabweichungen vermeiden.

Wenn Sie Kontrollen in aktivieren oder deaktivieren, gilt die Aktion für alle Konten und Regionen AWS Control Tower, die von verwaltet werden. AWS Control Tower Wenn Sie Kontrollen in Security Hub CSPM aktivieren und deaktivieren (für diesen Standard nicht empfohlen), gilt die Aktion nur für das aktuelle Konto und die Region.

> **Note**
>
> Die zentrale Konfiguration kann nicht zur Verwaltung von Service-Managed Standard: verwendet werden. AWS Control Tower Sie können nur den AWS Control Tower Dienst verwenden, um die Steuerungen in diesem Standard zu aktivieren und zu deaktivieren.

Aktivierungsstatus und Kontrollstatus anzeigen

Sie können den Aktivierungsstatus einer Kontrolle mit einer der folgenden Methoden anzeigen:

- Security Hub CSPM-Konsole, Security Hub CSPM-API oder AWS CLI
- AWS Control Tower Konsole
- AWS Control Tower API, um eine Liste der aktivierten Steuerelemente zu sehen (rufen Sie die `ListEnabledControls`API auf)
- AWS CLI um eine Liste der aktivierten Steuerelemente zu sehen (führen Sie den `list-enabled-controls`Befehl aus)

Ein Steuerelement, das Sie deaktivieren, AWS Control Tower hat den Aktivierungsstatus `Disabled` in Security Hub CSPM, sofern Sie dieses Steuerelement nicht explizit in Security Hub CSPM aktivieren.

Security Hub CSPM berechnet den Kontrollstatus auf der Grundlage des Workflow-Status und des Compliance-Status der Kontrollergebnisse. Weitere Informationen zum Aktivierungsstatus und zum Kontrollstatus finden Sie unter. Überprüfung der Details der Kontrollen in Security Hub CSPM

Auf der Grundlage des Kontrollstatus berechnet Security Hub CSPM eine Sicherheitsbewertung für Standard:. Service-Managed AWS Control Tower Diese Bewertung ist nur in Security Hub CSPM verfügbar. Darüber hinaus können Sie Kontrollergebnisse nur in Security Hub CSPM anzeigen. Die Standard-Sicherheitsbewertung und die Kontrollergebnisse sind in nicht verfügbar. AWS Control Tower

> **Note**
>
> Wenn Sie Kontrollen für Service-Managed Standard: aktivieren AWS Control Tower, kann es bis zu 18 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die eine bestehende AWS Config serviceverknüpfte Regel verwenden. Möglicherweise verfügen Sie bereits über serviceverknüpfte Regeln, wenn Sie andere Standards und Kontrollen in Security Hub CSPM aktiviert haben. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Den Standard löschen

Sie können diesen vom Dienst verwalteten Standard löschen, AWS Control Tower indem Sie alle entsprechenden Steuerelemente mit einer der folgenden Methoden deaktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die `DisableControl`API auf)
- AWS CLI (führe den `disable-control`Befehl aus)

Durch das Deaktivieren aller Steuerelemente wird der Standard in allen verwalteten Konten und kontrollierten Regionen in gelöscht. AWS Control Tower Wenn Sie den Standard-in löschen, wird er von der Seite Standards der Security Hub CSPM-Konsole AWS Control Tower entfernt, und Sie können nicht mehr mit der Security Hub CSPM-API darauf zugreifen oder. AWS CLI

> **Note**
>
> Durch die Deaktivierung aller Steuerelemente aus dem Standard in Security Hub CSPM wird der Standard nicht deaktiviert oder gelöscht.

Durch die Deaktivierung des Security Hub CSPM-Dienstes werden Service-Managed Standard: AWS Control Tower und alle anderen Standards, die Sie aktiviert haben, entfernt.

Das Feldformat für Standard finden: Service-Managed AWS Control Tower

Wenn Sie Service-Managed Standard: erstellen AWS Control Tower und Kontrollen dafür aktivieren, erhalten Sie ab sofort Kontrollergebnisse in Security Hub CSPM. Security Hub CSPM meldet Kontrollergebnisse in der. AWS Format für Sicherheitssuche (ASFF) Dies sind die ASFF-Werte für den Amazon Resource Name (ARN) dieses Standards und`GeneratorId`:

- Standard-ARN — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

Ein Beispielergebnis für Service-Managed Standard: AWS Control Tower finden Sie unterStichproben von Kontrollbefunden.

Kontrollen, die für Service-Managed Standard gelten: AWS Control Tower

Service-Managed Standard: AWS Control Tower unterstützt eine Untergruppe von Kontrollen, die Teil des FSBP-Standards (AWS Foundational Security Best Practices) sind. Wählen Sie ein Steuerelement aus, um Informationen darüber anzuzeigen, einschließlich Schritte zur Behebung fehlgeschlagener Ergebnisse.

Um zu sehen, von welchen Security Hub CSPM-Steuerelementen unterstützt werden AWS Control Tower, können Sie eine der folgenden Methoden verwenden:

- AWS Steuern Sie die Catalog-Konsole, nach der Sie filtern können `“Control owner = AWS Security Hub”`
- AWS Steuern Sie die Katalog-API (rufen Sie die `ListControls`API auf) mit dem Filter für`Implementations`, nach dem gesucht werden `Types` soll `AWS::SecurityHub::SecurityControl`

- AWS CLI (führe den `list-controls`Befehl aus) mit Filter für`Implementations`. Beispiel für einen CLI-Befehl:

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Regionale Grenzwerte für Security Hub CSPM-Steuerungen, wenn sie über den Control Tower Tower-Standard aktiviert sind, stimmen möglicherweise nicht mit den regionalen Grenzwerten für die zugrunde liegenden Kontrollen überein.

Wenn in Security Hub CSPM konsolidierte Kontrollergebnisse in Ihrem Konto deaktiviert sind, verwendet das `ProductFields.ControlId` Feld in den generierten Ergebnissen die standardbasierte Kontroll-ID. Die standardbasierte Kontroll-ID ist als CT formatiert. ***`ControlId`***(zum Beispiel). CT.CodeBuild.1

Weitere Informationen zu diesem Standard finden Sie unter Security Hub CSPM-Steuerelemente im AWS Control Tower Benutzerhandbuch.

Einen Sicherheitsstandard aktivieren

Wenn Sie einen Sicherheitsstandard in AWS Security Hub CSPM aktivieren, erstellt und aktiviert Security Hub CSPM automatisch alle Kontrollen, die für den Standard gelten. Security Hub CSPM beginnt auch mit der Durchführung von Sicherheitsprüfungen und der Generierung von Ergebnissen für die Kontrollen.

Um die Abdeckung und Genauigkeit der Ergebnisse zu optimieren, aktivieren und konfigurieren Sie die Ressourcenaufzeichnung, AWS Config bevor Sie einen Standard aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten. Weitere Informationen finden Sie unter Aktivierung und Konfiguration AWS Config für Security Hub CSPM.

Multi-Cloud-Sicherheitsstandards wie CIS Azure Foundations Benchmark v4.0.0 haben andere Anforderungen als Standards. AWS Multicloud-Standards erfordern einen Security Hub CSPM-Connector für den externen Cloud-Anbieter und erfordern nicht, dass Sie einen Konfigurationsrekorder konfigurieren AWS Config oder manuell erstellen. Der Security Hub CSPM Multicloud-Connector richtet automatisch einen serviceverknüpften Rekorder ein, um Ressourcen in der externen Cloud-Umgebung auszuwerten.

Nachdem Sie einen Standard aktiviert haben, können Sie einzelne Steuerungen, die für den Standard gelten, deaktivieren oder später wieder aktivieren. Wenn Sie ein Steuerelement für einen Standard deaktivieren, generiert Security Hub CSPM keine Ergebnisse mehr für das Steuerelement. Darüber hinaus ignoriert Security Hub CSPM das Steuerelement bei der Berechnung der Sicherheitsbewertung für den Standard. Die Sicherheitsbewertung ist der Prozentsatz der Kontrollen, die die Bewertung bestanden haben, im Verhältnis zur Gesamtzahl der Kontrollen, die für den Standard gelten, aktiviert sind und über Bewertungsdaten verfügen.

Wenn Sie einen Standard aktivieren, generiert Security Hub CSPM eine vorläufige Sicherheitsbewertung für den Standard, in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Seite Zusammenfassung oder Sicherheitsstandards auf der Security Hub CSPM-Konsole. Sicherheitsbewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten auf der Konsole aufrufen. Darüber hinaus muss die Ressourcenaufzeichnung konfiguriert sein, damit AWS Config die Punktzahlen angezeigt werden. In den China Regionen und kann es bis zu 24 Stunden dauern AWS GovCloud (US) Regions, bis Security Hub CSPM eine vorläufige Sicherheitsbewertung für einen Standard generiert. Nachdem Security Hub CSPM eine vorläufige Bewertung generiert hat, wird die Bewertung alle 24 Stunden aktualisiert. Um festzustellen, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde, können Sie sich auf einen Zeitstempel beziehen, den Security Hub CSPM für die Bewertung bereitstellt. Weitere Informationen finden Sie unter Berechnung der Sicherheitswerte.

Wie Sie einen Standard aktivieren, hängt davon ab, ob Sie die zentrale Konfiguration verwenden, um Security Hub CSPM für mehrere Konten zu verwalten und. AWS-Regionen Wir empfehlen die zentrale Konfiguration, wenn Sie Standards in Umgebungen mit mehreren Konten und mehreren Regionen aktivieren möchten. Sie können die zentrale Konfiguration verwenden, wenn Sie Security Hub CSPM mit integrieren. AWS Organizations Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie jeden Standard separat in jedem Konto und jeder Region aktivieren.

Themen

- Aktivierung eines Standards in mehreren Konten und AWS-Regionen
- Aktivierung eines Standards in einem einzigen Konto und AWS-Region
- Den Status eines Standards überprüfen

Aktivierung eines Standards in mehreren Konten und AWS-Regionen

Verwenden Sie die zentrale Konfiguration, um einen Sicherheitsstandard für mehrere Konten zu aktivieren und AWS-Regionen zu konfigurieren. Bei der zentralen Konfiguration kann der

delegierte Security Hub CSPM-Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards aktivieren. Der Administrator kann dann einzelnen Konten, Organisationseinheiten (OUs) oder dem Stammkonto eine Konfigurationsrichtlinie zuordnen. Eine Konfigurationsrichtlinie wirkt sich auf die Heimatregion, die auch als Aggregationsregion bezeichnet wird, und auf alle verknüpften Regionen aus.

Konfigurationsrichtlinien bieten Anpassungsoptionen. Sie können sich beispielsweise dafür entscheiden, nur den FSBP-Standard (AWS Foundational Security Best Practices) für eine Organisationseinheit zu aktivieren. Für eine andere Organisationseinheit können Sie sich dafür entscheiden, sowohl den FSBP-Standard als auch den Benchmark v1.4.0-Standard der Center for Internet Security (CIS) AWS Foundations zu aktivieren. Informationen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte von Ihnen angegebene Standards aktiviert, finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

Wenn Sie die zentrale Konfiguration verwenden, aktiviert Security Hub CSPM nicht automatisch Standards in neuen oder bestehenden Konten. Stattdessen gibt der Security Hub CSPM-Administrator an, welche Standards für verschiedene Konten aktiviert werden sollen, wenn er Security Hub CSPM-Konfigurationsrichtlinien für seine Organisation erstellt. Security Hub CSPM bietet eine empfohlene Konfigurationsrichtlinie, in der nur der FSBP-Standard aktiviert ist. Weitere Informationen finden Sie unter Arten von Konfigurationsrichtlinien.

> **Note**
>
> Der Security Hub CSPM-Administrator kann mithilfe von Konfigurationsrichtlinien jeden Standard außer dem vom AWS Control Tower Service verwalteten Standard aktivieren. Um diesen Standard zu aktivieren, muss der Administrator ihn direkt verwenden. AWS Control Tower Sie müssen außerdem einzelne Steuerungen in diesem Standard für ein zentral verwaltetes Konto aktivieren oder deaktivieren. AWS Control Tower

Wenn Sie möchten, dass einige Konten Standards für ihre eigenen Konten aktivieren und konfigurieren, kann der Security Hub CSPM-Administrator diese Konten als selbstverwaltete Konten kennzeichnen. Self-managed Konten müssen Standards in jeder Region separat aktivieren und konfigurieren.

Aktivierung eines Standards in einem einzigen Konto und AWS-Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie keine Konfigurationsrichtlinien verwenden, um Sicherheitsstandards zentral in mehreren

Konten zu aktivieren oder AWS-Regionen. Sie können jedoch einen Standard für ein einzelnes Konto und eine Region aktivieren. Sie können dies mithilfe der Security Hub CSPM-Konsole oder der Security Hub CSPM-API tun.

Security Hub CSPM console

Gehen Sie wie folgt vor, um mithilfe der Security Hub CSPM-Konsole einen Standard für ein Konto und eine Region zu aktivieren.

Um einen Standard in einem Konto und einer Region zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Standard aktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus. Auf der Seite Sicherheitsstandards sind alle Standards aufgeführt, die Security Hub CSPM derzeit unterstützt. Wenn Sie bereits einen Standard aktiviert haben, enthält der Abschnitt für den Standard die aktuelle Sicherheitsbewertung und zusätzliche Details zum Standard.
4. Wählen Sie im Abschnitt für den Standard, den Sie aktivieren möchten, die Option Standard aktivieren aus.

Um den Standard in weiteren Regionen zu aktivieren, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Security Hub CSPM API

Verwenden Sie den Vorgang, um einen Standard programmgesteuert in einem einzigen Konto und einer Region zu aktivieren. BatchEnableStandards Oder, wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den batch-enable-standardsBefehl aus.

Verwenden Sie in Ihrer Anfrage den `StandardsArn` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, den Sie aktivieren möchten. Geben Sie auch die Region an, für die sich Ihre Anfrage bezieht. Mit dem folgenden Befehl wird beispielsweise der FSBP-Standard (AWS Foundational Security Best Practices) aktiviert:

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
```

```
--region us-east-1
```

Wo *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* ist der ARN des FSBP-Standards in der Region USA Ost (Nord-Virginia), und *us-east-1* ist die Region, in der er aktiviert werden soll.

Um den ARN für einen Standard abzurufen, verwenden Sie den DescribeStandardsVorgang oder, falls Sie den verwenden AWS CLI, führen Sie den describe-standardsBefehl aus.

Um zunächst eine Liste der Standards zu überprüfen, die derzeit in Ihrem Konto aktiviert sind, können Sie den GetEnabledStandardsVorgang verwenden. Wenn Sie den verwenden AWS CLI, können Sie den Befehl get-enabled-standards ausführen, um diese Liste abzurufen.

Nachdem Sie einen Standard aktiviert haben, beginnt Security Hub CSPM mit der Ausführung von Aufgaben, um den Standard im Konto und in der angegebenen Region zu aktivieren. Dazu gehört die Erstellung aller Kontrollen, die für den Standard gelten. Um den Status dieser Aufgaben zu überwachen, können Sie den Status des Standards für das Konto und die Region überprüfen.

Den Status eines Standards überprüfen

Wenn Sie einen Sicherheitsstandard für ein Konto aktivieren, beginnt Security Hub CSPM mit der Erstellung aller Kontrollen, die für den Standard im Konto gelten. Security Hub CSPM führt auch zusätzliche Aufgaben aus, um den Standard für das Konto zu aktivieren, z. B. die Generierung einer vorläufigen Sicherheitsbewertung für den Standard. Während Security Hub CSPM diese Aufgaben ausführt, bezieht sich der Status des Standards auf das PendingKonto. Der Status des Standards durchläuft dann weitere Status, die Sie überwachen und überprüfen können.

> **Note**
>
> Änderungen an einzelnen Kontrollen für eine Norm wirken sich nicht auf den Gesamtstatus der Norm aus. Wenn Sie beispielsweise ein Steuerelement aktivieren, das Sie zuvor deaktiviert haben, wirkt sich Ihre Änderung nicht auf den Status des Standards aus. Ebenso wirkt sich Ihre Änderung nicht auf den Status des Standards aus, wenn Sie einen Parameterwert für ein aktiviertes Steuerelement ändern.

Um den Status eines Standards mithilfe der Security Hub CSPM-Konsole zu überprüfen, wählen Sie im Navigationsbereich Sicherheitsstandards aus. Auf der Seite Sicherheitsstandards sind alle Standards aufgeführt, die Security Hub CSPM derzeit unterstützt. Wenn Security Hub CSPM derzeit

Aufgaben zur Aktivierung des Standards ausführt, gibt der Abschnitt für den Standard an, dass Security Hub CSPM immer noch eine Sicherheitsbewertung für den Standard generiert. Wenn ein Standard aktiviert ist, enthält der Abschnitt für den Standard die aktuelle Bewertung. Wählen Sie Ergebnisse anzeigen, um zusätzliche Details zu überprüfen, einschließlich des Status einzelner Kontrollen, die für den Standard gelten. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Verwenden Sie den Vorgang, um den Status eines Standards programmgesteuert mit der Security Hub CSPM-API zu überprüfen. GetEnabledStandards Verwenden Sie in Ihrer Anfrage optional den `StandardsSubscriptionArns` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, dessen Status Sie überprüfen möchten. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, können Sie den Befehl get-enabled-standards ausführen, um den Status eines Standards zu überprüfen. Verwenden Sie den `standards-subscription-arns` Parameter, um den ARN des zu prüfenden Standards anzugeben. Um zu ermitteln, welcher ARN angegeben werden soll, können Sie den DescribeStandardsVorgang verwenden oder für den den AWS CLI den describe-standardsBefehl ausführen.

Wenn Ihre Anfrage erfolgreich ist, antwortet Security Hub CSPM mit einer Reihe von Objekten. `StandardsSubscription` Ein Standardabonnement ist eine AWS Ressource, die Security Hub CSPM in einem Konto erstellt, wenn ein Standard für das Konto aktiviert ist. Jedes `StandardsSubscription` Objekt enthält Details zu einem Standard, der derzeit für das Konto aktiviert ist oder gerade aktiviert oder deaktiviert wird. In jedem Objekt gibt das `StandardsStatus` Feld den aktuellen Status des Standards für das Konto an.

Der Status eines Standards (`StandardsStatus`) kann einer der folgenden sein.

PENDING

> Security Hub CSPM führt derzeit Aufgaben aus, um den Standard für das Konto zu aktivieren. Dazu gehören die Erstellung der Kontrollen, die für den Standard gelten, und die Erstellung einer vorläufigen Sicherheitsbewertung für den Standard. Es kann mehrere Minuten dauern, bis Security Hub CSPM alle Aufgaben abgeschlossen hat. Ein Standard kann diesen Status auch haben, wenn er bereits für das Konto aktiviert ist und Security Hub CSPM dem Standard derzeit neue Steuerungen hinzufügt.
>
> Wenn ein Standard diesen Status hat, können Sie möglicherweise nicht die Details einzelner Kontrollen abrufen, die für den Standard gelten. Darüber hinaus sind Sie möglicherweise nicht in der Lage, einzelne Steuerelemente für den Standard zu konfigurieren oder zu deaktivieren. Wenn

Sie beispielsweise versuchen, ein Steuerelement mithilfe des UpdateStandardsControlVorgangs zu deaktivieren, tritt ein Fehler auf.

Anhand des Werts für das `StandardsControlsUpdatable` Feld können Sie feststellen, ob Sie einzelne Steuerelemente für den Standard konfigurieren oder anderweitig verwalten können. Wenn der Wert für dieses Feld lautet`READY_FOR_UPDATES`, können Sie mit der Verwaltung einzelner Steuerelemente für den Standard beginnen. Warten Sie andernfalls, bis Security Hub CSPM zusätzliche Verarbeitungsaufgaben abgeschlossen hat, um den Standard zu aktivieren.

READY

Der Standard ist derzeit für das Konto aktiviert. Security Hub CSPM kann Sicherheitsprüfungen durchführen und Ergebnisse für alle Kontrollen generieren, die für den Standard gelten und derzeit aktiviert sind. Security Hub CSPM kann auch eine Sicherheitsbewertung für den Standard berechnen.

Wenn ein Standard diesen Status hat, können Sie die Details der einzelnen Kontrollen abrufen, die für den Standard gelten. Darüber hinaus können Sie die Steuerelemente konfigurieren, deaktivieren oder erneut aktivieren. Sie können den Standard auch deaktivieren.

INCOMPLETE

Security Hub CSPM konnte den Standard für das Konto nicht vollständig aktivieren. Security Hub CSPM kann keine Sicherheitsprüfungen durchführen und keine Ergebnisse für alle Kontrollen generieren, die für den Standard gelten und derzeit aktiviert sind. Darüber hinaus kann Security Hub CSPM keine Sicherheitsbewertung für den Standard berechnen.

Bei Multicloud-Standards wird das Abonnement `INCOMPLETE` mit dem Status „`NO_AVAILABLE_MULTICLOUD_CONNECTOR`Wenn Sie den Standard ohne CSPM-Connector aktivieren“ eingegeben. Das Abonnement wechselt automatisch zu dem `READY` Zeitpunkt, zu dem ein Connector verfügbar ist.

Anhand der Informationen im `StandardsStatusReason` Array können Sie ermitteln, warum der Standard nicht vollständig aktiviert werden konnte. Dieses Array spezifiziert Probleme, die Security Hub CSPM daran gehindert haben, den Standard zu aktivieren. Wenn ein interner Fehler aufgetreten ist, versuchen Sie erneut, den Standard für das Konto zu aktivieren. Bei anderen Problemen überprüfen Sie Ihre AWS Config Einstellungen. Sie können auch einzelne Steuerelemente deaktivieren, die Sie nicht überprüfen möchten, oder den Standard vollständig deaktivieren.

DELETING

Security Hub CSPM bearbeitet derzeit eine Anfrage zur Deaktivierung des Standards für das Konto. Dazu gehören die Deaktivierung der Kontrollen, die für den Standard gelten, und das Entfernen der zugehörigen Sicherheitsbewertung. Es kann mehrere Minuten dauern, bis Security Hub CSPM die Bearbeitung der Anfrage abgeschlossen hat.

Wenn ein Standard diesen Status hat, können Sie den Standard nicht erneut aktivieren oder erneut versuchen, ihn für das Konto zu deaktivieren. Security Hub CSPM muss zuerst die Bearbeitung der aktuellen Anfrage abschließen. Darüber hinaus können Sie die Details einzelner Kontrollen, die für den Standard gelten, nicht abrufen oder die Kontrollen verwalten.

FAILED

Security Hub CSPM konnte den Standard für das Konto nicht deaktivieren. Ein oder mehrere Fehler traten auf, als Security Hub CSPM versuchte, den Standard zu deaktivieren. Darüber hinaus kann Security Hub CSPM keine Sicherheitsbewertung für den Standard berechnen.

Anhand der Informationen im Array können Sie feststellen, warum der Standard nicht vollständig deaktiviert wurde. `StandardsStatusReason` Dieses Array spezifiziert Probleme, die Security Hub CSPM daran gehindert haben, den Standard zu deaktivieren.

Wenn ein Standard diesen Status hat, können Sie die Details einzelner Kontrollen, die für den Standard gelten, nicht abrufen oder die Kontrollen verwalten. Sie können den Standard jedoch für das Konto wieder aktivieren. Wenn Sie die Probleme beheben, die Security Hub CSPM daran gehindert haben, den Standard zu deaktivieren, können Sie auch erneut versuchen, den Standard zu deaktivieren.

Wenn der Status eines Standards lautet`READY`, führt Security Hub CSPM Sicherheitsprüfungen durch und generiert Ergebnisse für alle Kontrollen, die für den Standard gelten und derzeit aktiviert sind. Bei anderen Status führt Security Hub CSPM möglicherweise Prüfungen durch und generiert Ergebnisse für einige, aber nicht alle aktivierten Kontrollen. Es kann bis zu 24 Stunden dauern, bis die Kontrollergebnisse generiert oder aktualisiert werden. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Überprüfung der Einzelheiten eines Sicherheitsstandards

Nachdem Sie einen Sicherheitsstandard in AWS Security Hub CSPM aktiviert haben, können Sie die Konsole verwenden, um die Details des Standards zu überprüfen. Auf der Konsole enthält die Detailseite für einen Standard die folgenden Informationen:

- Die aktuelle Sicherheitsbewertung für den Standard.
- Eine Tabelle mit Kontrollen, die für den Standard gelten.
- Aggregierte Statistiken für Kontrollen, die für den Standard gelten.
- Eine visuelle Zusammenfassung des Status der Kontrollen, die für den Standard gelten.
- Eine visuelle Zusammenfassung der Sicherheitsprüfungen für Kontrollen, die aktiviert sind und dem Standard entsprechen. Bei der Integration mit gelten Steuerelemente AWS Organizations, die in mindestens einem Organisationskonto aktiviert sind, als aktiviert.

Um diese Details zu überprüfen, wählen Sie im Navigationsbereich der Konsole Sicherheitsstandards aus. Wählen Sie dann im Abschnitt für den Standard die Option Ergebnisse anzeigen aus. Für eine eingehendere Analyse können Sie die Daten filtern und sortieren und sich die Details der einzelnen Kontrollen ansehen, die für den Standard gelten.

Themen

- Grundlegendes zur Standard-Sicherheitsbewertung
- Überprüfung der Kontrollen im Hinblick auf einen Standard

Grundlegendes zur Standard-Sicherheitsbewertung

Auf der AWS Security Hub CSPM-Konsole wird auf der Detailseite für einen Standard die Sicherheitsbewertung für den Standard angezeigt. Die Punktzahl ist der Prozentsatz der Kontrollen, die die Bewertung bestanden haben, im Verhältnis zur Gesamtzahl der Kontrollen, die für den Standard gelten, aktiviert sind und über Bewertungsdaten verfügen. Unter der Punktzahl befindet sich ein Diagramm, das die Sicherheitsüberprüfungen für Kontrollen zusammenfasst, die für den Standard aktiviert sind. Dies beinhaltet die Anzahl der bestandenen und fehlgeschlagenen Sicherheitsprüfungen. Bei Administratorkonten werden die Standardpunktzahl und das Diagramm für das Administratorkonto und alle Mitgliedskonten zusammengefasst. Um fehlgeschlagene Sicherheitsüberprüfungen auf Kontrollen mit einem bestimmten Schweregrad zu überprüfen, wählen Sie den Schweregrad aus.

Wenn Sie einen Standard aktivieren, generiert Security Hub CSPM eine vorläufige Sicherheitsbewertung für den Standard, in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden,

damit die Ergebnisse angezeigt werden. In den Regionen China und kann es bis zu 24 Stunden dauern AWS GovCloud (US) Regions, bis Security Hub CSPM eine vorläufige Bewertung generiert. Nachdem Security Hub CSPM eine vorläufige Bewertung für einen Standard generiert hat, wird die Bewertung alle 24 Stunden aktualisiert. Weitere Informationen finden Sie unter Berechnung der Sicherheitswerte.

Alle Daten auf den Detailseiten zu Sicherheitsstandards beziehen sich auf den aktuellen Stand, AWS-Region sofern Sie keine Aggregationsregion festlegen. Wenn Sie eine Aggregationsregion festlegen, gelten die Sicherheitsbewertungen für alle Regionen und beinhalten Ergebnisse für alle verknüpften Regionen. Darüber hinaus spiegelt der Konformitätsstatus der Kontrollen Ergebnisse aus verknüpften Regionen wider, und die Anzahl der Sicherheitsprüfungen umfasst Ergebnisse aus verknüpften Regionen.

Überprüfung der Kontrollen im Hinblick auf einen Standard

Wenn Sie die AWS Security Hub CSPM-Konsole verwenden, um die Details eines Standards zu überprüfen, den Sie aktiviert haben, können Sie eine Tabelle mit Sicherheitskontrollen überprüfen, die für den Standard gelten. Für jedes Steuerelement enthält die Tabelle die folgenden Informationen:

- Die Kontroll-ID und der Titel.
- Der Status des Steuerelements. Weitere Informationen finden Sie unter Bewertung des Konformitätsstatus und des Kontrollstatus.
- Der Schweregrad, der der Kontrolle zugewiesen wurde.
- Die Anzahl der fehlgeschlagenen Prüfungen und die Gesamtzahl der Prüfungen. Falls zutreffend, gibt das Feld Fehlgeschlagene Prüfungen auch die Anzahl der Ergebnisse mit dem Status Unbekannt an.
- Ob das Steuerelement benutzerdefinierte Parameter unterstützt. Weitere Informationen finden Sie unter Grundlegendes zu den Steuerungsparametern in Security Hub CSPM.

Security Hub CSPM-Updates kontrollieren den Status und die Anzahl der Sicherheitschecks alle 24 Stunden. Ein Zeitstempel oben auf der Seite gibt an, wann Security Hub CSPM diese Daten zuletzt aktualisiert hat.

Bei Administratorkonten werden der Kontrollstatus und die Anzahl der Sicherheitsüberprüfungen für das Administratorkonto und alle Mitgliedskonten zusammengefasst. Die Anzahl der aktivierten Steuerelemente umfasst Kontrollen, die standardmäßig im Administratorkonto oder in mindestens einem Mitgliedskonto aktiviert sind. Die Anzahl der deaktivierten Steuerelemente umfasst

Steuerelemente, die standardmäßig im Administratorkonto und in allen Mitgliedskonten deaktiviert sind.

Sie können die Tabelle mit den Steuerelementen filtern, die für den Standard gelten. Mithilfe der Optionen „Nach filtern“ neben der Tabelle können Sie wählen, ob nur aktivierte oder nur deaktivierte Steuerelemente für den Standard angezeigt werden sollen. Wenn Sie nur aktivierte Steuerelemente anzeigen, können Sie die Tabelle weiter nach dem Status der Steuerelemente filtern. Sie können sich dann auf Steuerelemente konzentrieren, die einen bestimmten Kontrollstatus haben. Zusätzlich zu den Optionen Filtern nach können Sie Filterkriterien in das Feld Steuerelemente filtern eingeben. Sie können beispielsweise nach der Kontroll-ID oder dem Titel filtern.

Wählen Sie Ihre bevorzugte Zugriffsmethode. Folgen Sie dann den Schritten, um die Kontrollen zu überprüfen, die für einen von Ihnen aktivierten Standard gelten.

Security Hub CSPM console

Um die Steuerelemente für einen aktivierten Standard zu überprüfen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus.
3. Wählen Sie im Abschnitt für den Standard die Option Ergebnisse anzeigen aus.

In der Tabelle unten auf der Seite sind alle Steuerelemente aufgeführt, die für den Standard gelten. Sie können die Tabelle filtern und sortieren. Sie können die aktuelle Seite der Tabelle auch als CSV-Datei herunterladen. Wählen Sie dazu oberhalb der Tabelle die Option Herunterladen aus. Wenn Sie die Tabelle filtern, enthält die heruntergeladene Datei nur die Steuerelemente, die Ihren aktuellen Filtereinstellungen entsprechen.

Security Hub CSPM API

Um die Steuerelemente für einen aktivierten Standard zu überprüfen

1. Verwenden Sie den ListSecurityControlDefinitionsBetrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den Befehl list-security-control-definitions aus.

   Geben Sie den Amazon-Ressourcennamen (ARN) des Standards an, für den Sie die Kontrollen überprüfen möchten. Um ARNs für Standards zu erhalten, verwenden Sie den DescribeStandardsVorgang oder führen Sie den Befehl describe-standards aus. Wenn Sie

den ARN für einen Standard nicht angeben, gibt Security Hub CSPM alle Security Control IDs zurück.

2. Verwenden Sie den ListStandardsControlAssociationsBetrieb der Security Hub CSPM-API oder führen Sie den Befehl list-standards-control-associations aus. Dieser Vorgang gibt an, in welchen Standards ein Steuerelement aktiviert ist.

   Identifizieren Sie das Steuerelement, indem Sie die Sicherheitskontroll-ID oder den ARN angeben. Paginierungsparameter sind optional.

Im folgenden Beispiel erfahren Sie, in welchen Standards das Config.1 Steuerelement aktiviert ist.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Beim Ausschalten automatisch aktivierter Sicherheitsstandards

Wenn Ihre Organisation keine zentrale Konfiguration verwendet, verwendet sie einen Konfigurationstyp, der als lokale Konfiguration bezeichnet wird. Mit der lokalen Konfiguration kann AWS Security Hub CSPM automatisch Standardsicherheitsstandards für neue Mitgliedskonten aktivieren, wenn die Konten Ihrer Organisation beitreten. Alle Kontrollen, die für diese Standardstandards gelten, werden ebenfalls automatisch aktiviert.

Derzeit sind die Standardsicherheitsstandards der Standard AWS Foundation Security Best Practices und der Benchmark v1.2.0-Standard der Center for Internet Security (CIS) AWS Foundations. Informationen zu diesen Standards finden Sie im. Standardreferenz für Security Hub CSPM

Wenn Sie Sicherheitsstandards für neue Mitgliedskonten lieber manuell aktivieren möchten, können Sie die automatische Aktivierung der Standardstandards deaktivieren. Dies ist nur möglich, wenn Sie die lokale Konfiguration integrieren AWS Organizations und diese verwenden. Wenn Sie die zentrale Konfiguration verwenden, können Sie stattdessen eine Konfigurationsrichtlinie erstellen, die die Standardstandards aktiviert, und die Richtlinie dem Stammverzeichnis zuordnen. Alle Ihre Organisationskonten und Organisationseinheiten erben dann diese Konfigurationsrichtlinie, sofern sie nicht mit einer anderen Richtlinie verknüpft sind oder selbst verwaltet werden. Wenn Sie nicht integrieren AWS Organizations, können Sie einen Standardstandard deaktivieren, wenn Sie Security Hub CSPM zum ersten Mal oder später aktivieren. Um zu erfahren wie dies geht, vgl. Deaktivierung eines Standards.

Um die automatische Aktivierung der Standardstandards für neue Mitgliedskonten zu deaktivieren, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Security Hub CSPM console

Gehen Sie wie folgt vor, um die automatische Aktivierung der Standardstandards mithilfe der Security Hub CSPM-Konsole zu deaktivieren.

Um die automatische Aktivierung von Standardstandards zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Übersicht die Option Bearbeiten aus.
4. Deaktivieren Sie unter Neue Kontoeinstellungen das Kontrollkästchen Standardsicherheitsstandards aktivieren.
5. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Um die automatische Aktivierung der Standardstandards programmgesteuert zu deaktivieren, verwenden Sie vom Security Hub CSPM-Administratorkonto aus den UpdateOrganizationConfigurationBetrieb der Security Hub CSPM-API. Geben Sie in Ihrer Anfrage den Parameter an. `NONE` `AutoEnableStandards`

Wenn Sie den verwenden AWS CLI, führen Sie den update-organization-configurationBefehl aus, um die automatische Aktivierung der Standardstandards zu deaktivieren. Geben Sie für den Parameter `auto-enable-standards` `NONE` an: Der folgende Befehl aktiviert beispielsweise automatisch Security Hub CSPM für neue Mitgliedskonten und deaktiviert die automatische Aktivierung der Standardstandards für die Konten.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-
standards NONE
```

Deaktivierung eines Sicherheitsstandards

Wenn Sie einen Sicherheitsstandard in AWS Security Hub CSPM deaktivieren, passiert Folgendes:

- Alle Steuerelemente, die für den Standard gelten, sind deaktiviert, sofern sie nicht mit einem anderen Standard verknüpft sind, der derzeit aktiviert ist.
- Sicherheitsprüfungen für die deaktivierten Steuerelemente werden nicht mehr durchgeführt, und es werden keine weiteren Ergebnisse für die deaktivierten Steuerelemente generiert.
- Bestehende Ergebnisse für die deaktivierten Kontrollen werden nach etwa 3-5 Tagen automatisch archiviert.
- AWS Config Regeln, die Security Hub CSPM für die deaktivierten Steuerelemente erstellt hat, werden gelöscht.

Das Löschen der entsprechenden AWS Config Regeln erfolgt in der Regel innerhalb weniger Minuten nach der Deaktivierung eines Standards. Es kann jedoch länger dauern. Wenn die erste Anfrage die Regeln nicht löscht, versucht Security Hub CSPM alle 12 Stunden erneut. Wenn Sie Security Hub CSPM jedoch deaktiviert haben oder keine anderen Standards aktiviert haben, kann Security Hub CSPM es nicht erneut versuchen, was bedeutet, dass die Regeln nicht gelöscht werden können. Wenn dies der Fall ist und Sie die Regeln löschen müssen, wenden Sie sich an. AWS Support

> **Note**
>
> Die Deaktivierung eines Standards kann die mit der Deaktivierung der zugehörigen Regeln verbundenen AWS Config Kosten in die Höhe treiben. Bevor Sie Standards deaktivieren, empfehlen wir Ihnen, die Dokumentation Überlegungen zum Löschen von AWS Config Regeln zu lesen. Lesen Sie auch, wie Sie Resource Compliance-Konfigurationselemente von der Aufzeichnung ausschließen können, wenn Regeln, die an einen Security Hub CSPM-Standard gebunden sind, deaktiviert sind.

Themen

- Deaktivierung eines Standards in mehreren Konten und AWS-Regionen
- Deaktivierung eines Standards in einem einzelnen Konto und AWS-Region

Deaktivierung eines Standards in mehreren Konten und AWS-Regionen

Verwenden Sie die zentrale Konfiguration AWS-Regionen, um einen Sicherheitsstandard für mehrere Konten und zu deaktivieren. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards deaktivieren. Der Administrator kann dann einzelnen Konten, Organisationseinheiten (OUs) oder dem Stammkonto eine Konfigurationsrichtlinie zuordnen. Eine Konfigurationsrichtlinie wirkt sich auf die Heimatregion, die auch als Aggregationsregion bezeichnet wird, und auf alle verknüpften Regionen aus.

Konfigurationsrichtlinien bieten Anpassungsoptionen. Sie könnten sich beispielsweise dafür entscheiden, den Payment Card Industry Data Security Standard (PCI DSS) in einer Organisationseinheit zu deaktivieren. Für eine andere Organisationseinheit könnten Sie sich dafür entscheiden, sowohl den PCI DSS als auch den Standard SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) zu deaktivieren. Informationen zum Erstellen einer Konfigurationsrichtlinie, mit der einzelne von Ihnen angegebene Standards aktiviert oder deaktiviert werden, finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

> **Note**
>
> Der Security Hub CSPM-Administrator kann mithilfe von Konfigurationsrichtlinien jeden Standard außer dem vom AWS Control Tower Service verwalteten Standard deaktivieren. Um diesen Standard zu deaktivieren, muss der Administrator ihn direkt verwenden. AWS Control Tower Sie müssen außerdem einzelne Steuerungen in diesem Standard für ein zentral verwaltetes Konto verwenden, AWS Control Tower um sie zu deaktivieren oder zu aktivieren.

Wenn Sie möchten, dass einige Konten Standards für ihre eigenen Konten konfigurieren oder deaktivieren, kann der Security Hub CSPM-Administrator diese Konten als selbstverwaltete Konten kennzeichnen. Self-managed Konten müssen die Standards in jeder Region separat deaktivieren.

Deaktivierung eines Standards in einem einzelnen Konto und AWS-Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie keine Konfigurationsrichtlinien verwenden, um Sicherheitsstandards in mehreren Konten zentral zu deaktivieren oder. AWS-Regionen Sie können jedoch einen Standard für ein einzelnes Konto und eine Region deaktivieren. Sie können dies mithilfe der Security Hub CSPM-Konsole oder der Security Hub CSPM-API tun.

Security Hub CSPM console

Gehen Sie wie folgt vor, um einen Standard in einem Konto und einer Region mithilfe der Security Hub CSPM-Konsole zu deaktivieren.

Um einen Standard in einem Konto und einer Region zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Standard deaktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus.
4. Wählen Sie im Abschnitt für den Standard, den Sie deaktivieren möchten, die Option Standard deaktivieren aus.

Um den Standard in weiteren Regionen zu deaktivieren, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Security Hub CSPM API

Verwenden Sie den Vorgang, um einen Standard programmgesteuert in einem einzelnen Konto und einer Region zu deaktivieren. BatchDisableStandards Oder, wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den batch-disable-standardsBefehl aus.

Verwenden Sie in Ihrer Anfrage den `StandardsSubscriptionArns` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, den Sie deaktivieren möchten. Wenn Sie den verwenden AWS CLI, verwenden Sie den `standards-subscription-arns` Parameter, um den ARN anzugeben. Geben Sie auch die Region an, für die sich Ihre Anfrage bezieht. Mit dem folgenden Befehl wird beispielsweise der FSBP-Standard (AWS Foundational Security Best Practices) für ein Konto () deaktiviert: *123456789012*

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Wo *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* ist der ARN des FSBP-Standards

für das Konto in der Region USA Ost (Nord-Virginia), und `us-east-1` ist die Region, in der es deaktiviert werden soll.

Um den ARN für einen Standard zu erhalten, können Sie die GetEnabledStandardsOperation verwenden. Bei diesem Vorgang werden Informationen zu den Standards abgerufen, die derzeit in Ihrem Konto aktiviert sind. Wenn Sie den verwenden AWS CLI, können Sie den Befehl get-enabled-standards ausführen, um diese Informationen abzurufen.

Nachdem Sie einen Standard deaktiviert haben, beginnt Security Hub CSPM mit der Ausführung von Aufgaben zur Deaktivierung des Standards im Konto und in der angegebenen Region. Dazu gehört auch die Deaktivierung aller Kontrollen, die für den Standard gelten. Um den Status dieser Aufgaben zu überwachen, können Sie den Status des Standards für das Konto und die Region überprüfen.

Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM

In AWS Security Hub CSPM ist eine Sicherheitskontrolle, auch Kontrolle genannt, eine Schutzmaßnahme innerhalb eines Sicherheitsstandards, die einer Organisation hilft, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Informationen zu schützen. In Security Hub CSPM bezieht sich eine Kontrolle auf eine bestimmte Ressource. AWS

Wenn Sie ein Steuerelement in einem oder mehreren Standards aktivieren, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsprüfungen für dieses Steuerelement. Die Sicherheitsprüfungen führen zu Ergebnissen von Security Hub CSPM. Wenn Sie ein Steuerelement deaktivieren, beendet Security Hub CSPM die Durchführung von Sicherheitsüberprüfungen für dieses Steuerelement und es werden keine Ergebnisse mehr generiert.

Sie können Steuerelemente einzeln für ein einzelnes Konto aktivieren oder deaktivieren und. AWS-Region Um Zeit zu sparen und Konfigurationsabweichungen in Umgebungen mit mehreren Konten zu reduzieren, empfehlen wir, die zentrale Konfiguration zu verwenden, um Steuerelemente zu aktivieren oder zu deaktivieren. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Richtlinien erstellen, die festlegen, wie eine Steuerung für mehrere Konten und Regionen konfiguriert werden soll. Weitere Informationen zum Aktivieren und Deaktivieren von Steuerelementen finden Sie unter. Steuerelemente in Security Hub CSPM aktivieren

Ansicht „Konsolidierte Steuerelemente“

Auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole werden alle in der aktuellen Version verfügbaren Steuerelemente angezeigt AWS-Region (Sie können die Steuerelemente im Kontext

eines Standards anzeigen, indem Sie die Seite „Sicherheitsstandards“ aufrufen und einen aktivierten Standard auswählen). Security Hub CSPM weist den Kontrollen standardübergreifend eine einheitliche Sicherheitskontroll-ID, einen Titel und eine Beschreibung zu. Die Kontrollen-IDs enthalten die entsprechende AWS-Service und eine eindeutige Nummer (z. B.). CodeBuild.3

Die folgenden Informationen sind auf der Seite „Steuerelemente“ der Security Hub CSPM-Konsole verfügbar:

- Eine allgemeine Sicherheitsbewertung, die auf dem Anteil der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit Daten basiert
- Aufschlüsselung des Kontrollstatus aller unterstützten Security Hub CSPM-Steuerelemente
- Die Gesamtzahl der bestandenen und nicht bestandenen Sicherheitsprüfungen.
- Die Anzahl der fehlgeschlagenen Sicherheitsprüfungen für Kontrollen mit unterschiedlichem Schweregrad sowie Links zu weiteren Details zu diesen fehlgeschlagenen Prüfungen.
- Eine Liste der Security Hub CSPM-Steuerelemente mit Filtern zur Anzeige bestimmter Untergruppen von Kontrollen.

Auf der Seite „Kontrollen“ können Sie ein Steuerelement auswählen, um dessen Details anzuzeigen und anhand der von der Kontrolle generierten Ergebnisse Maßnahmen zu ergreifen. Auf dieser Seite können Sie auch eine Sicherheitskontrolle in Ihrem aktuellen AWS-Konto und aktivieren oder deaktivieren AWS-Region. Die Aktivierungs- und Deaktivierungsaktionen auf der Seite „Kontrollen“ gelten für alle Standards. Weitere Informationen finden Sie unter Steuerelemente in Security Hub CSPM aktivieren.

Bei Administratorkonten gibt die Seite „Kontrollen“ den Status der Kontrollen in den Mitgliedskonten wieder. Schlägt eine Kontrollprüfung in mindestens einem Mitgliedskonto fehl, lautet der Kontrollstatus Fehlgeschlagen. Wenn Sie eine Aggregationsregion festgelegt haben, wird auf der Seite „Kontrollen“ der Status der Kontrollen in allen verknüpften Regionen angezeigt. Wenn eine Kontrollprüfung in mindestens einer verknüpften Region fehlschlägt, lautet der Kontrollstatus „Fehlgeschlagen“.

Die konsolidierte Ansicht der Kontrollen führt zu Änderungen an der Steuerung, nach Feldern im AWS Security Finding Format (ASFF) zu suchen, die sich auf Workflows auswirken können. Weitere Informationen finden Sie unter Ansicht konsolidierter Kontrollen — ASFF-Änderungen.

Zusammenfassung der Sicherheitsbewertung für Kontrollen

Auf der Seite „Kontrollen“ wird eine Zusammenfassung der Sicherheitsbewertung von 0 bis 100 Prozent angezeigt. Die zusammenfassende Sicherheitsbewertung wird auf der Grundlage des Anteils der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit Daten aus verschiedenen Standards berechnet.

> **Note**
>
> Um die allgemeine Sicherheitsbewertung für Kontrollen einzusehen, müssen Sie der IAM-Rolle, die Sie für den **`BatchGetControlEvaluations`** Zugriff auf Security Hub CSPM verwenden, die Berechtigung zum Aufrufen hinzufügen. Diese Berechtigung ist nicht erforderlich, um die Sicherheitsbewertungen für bestimmte Standards einzusehen.

Wenn Sie Security Hub CSPM aktivieren, berechnet Security Hub CSPM die anfängliche Sicherheitsbewertung innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Es kann bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen in den Regionen China und generiert werden. AWS GovCloud (US) Regions

Zusätzlich zur allgemeinen Sicherheitsbewertung berechnet Security Hub CSPM innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite mit den Sicherheitsstandards eine Standardsicherheitsbewertung für jeden aktivierten Standard. Verwenden Sie den API-Vorgang, um eine Liste der derzeit aktivierten Standards anzuzeigen. `GetEnabledStandards`

AWS Config muss für die Ressourcenaufzeichnung aktiviert sein, damit die Ergebnisse angezeigt werden. Informationen darüber, wie Security Hub CSPM Sicherheitsbewertungen berechnet, finden Sie unter. Berechnung der Sicherheitswerte

Nach der ersten Ergebnisgenerierung aktualisiert Security Hub CSPM die Sicherheitsbewertungen alle 24 Stunden. Security Hub CSPM zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde.

Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt die Gesamtsicherheitsbewertung die Kontrollergebnisse in den verknüpften Regionen wider.

Kontrollreferenz für Security Hub CSPM

Diese Kontrollreferenz enthält eine Tabelle der verfügbaren AWS Security Hub CSPM-Steuerelemente mit Links zu weiteren Informationen zu den einzelnen Steuerelementen. In der Tabelle sind die Kontrollen in alphabetischer Reihenfolge nach der Kontroll-ID aufgeführt. Nur Steuerelemente, die von Security Hub CSPM aktiv verwendet werden, sind hier enthalten. Steuerelemente, die nicht mehr verwendet wurden, sind in der Tabelle nicht enthalten.

Die Tabelle enthält die folgenden Informationen für jedes Steuerelement:

- ID der Sicherheitskontrolle — Diese ID gilt für alle Standards und gibt die AWS-Service Ressource an, auf die sich die Kontrolle bezieht. Die Security Hub CSPM-Konsole zeigt Security Control IDs an, unabhängig davon, ob Consolidated Control Findings in Ihrem Konto aktiviert oder deaktiviert ist. Die CSPM-Ergebnisse von Security Hub verweisen jedoch nur dann auf Sicherheitskontroll-IDs, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn konsolidierte Kontrollbefunde in Ihrem Konto deaktiviert sind, variieren einige Kontroll-IDs je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung von standardspezifischen Kontroll-IDs zu Sicherheitskontroll-IDs finden Sie unter. Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt

  Wenn Sie Automatisierungen für Sicherheitskontrollen einrichten möchten, empfehlen wir, anhand der Kontroll-ID und nicht anhand des Titels oder der Beschreibung zu filtern. Security Hub CSPM kann zwar gelegentlich Titel oder Beschreibungen von Steuerelementen aktualisieren, die Kontroll-IDs bleiben jedoch unverändert.

  Bei Kontroll-IDs können Zahlen übersprungen werden. Dies sind Platzhalter für future Kontrollen.
- Titel der Sicherheitskontrolle — Dieser Titel gilt für alle Standards. Die Security Hub CSPM-Konsole zeigt Titel für Sicherheitskontrollen an, unabhängig davon, ob konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert oder deaktiviert sind. Die CSPM-Ergebnisse von Security Hub verweisen jedoch nur dann auf Titel der Sicherheitskontrolle, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn die Option „Konsolidierte Kontrollbefunde“ in Ihrem Konto deaktiviert ist, variieren einige Kontrolltitel je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung von standardspezifischen Kontroll-IDs zu Sicherheitskontroll-IDs finden Sie unter. Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt
- Anwendbare Standards — Gibt an, für welche Standards eine Kontrolle gilt. Wählen Sie eine Kontrolle aus, um bestimmte Anforderungen aus Compliance-Frameworks von Drittanbietern zu überprüfen.

- Schweregrad — Der Schweregrad einer Kontrolle gibt an, wie wichtig sie aus Sicherheitsgründen ist. Informationen darüber, wie Security Hub CSPM den Schweregrad der Kontrolle bestimmt, finden Sie unter. Schweregrade der Kontrollbefunde
- Unterstützt benutzerdefinierte Parameter — Gibt an, ob das Steuerelement benutzerdefinierte Werte für einen oder mehrere Parameter unterstützt. Wählen Sie ein Steuerelement aus, um die Parameterdetails zu überprüfen. Weitere Informationen finden Sie unter Grundlegendes zu den Steuerungsparametern in Security Hub CSPM.
- Zeitplantyp — Gibt an, wann die Kontrolle ausgewertet wird. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Wählen Sie ein Steuerelement aus, um weitere Details zu überprüfen. Die Kontrollen werden in alphabetischer Reihenfolge nach der Sicherheitskontroll-ID aufgelistet.

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Account.1	Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
Account.2	AWS-Konto sollte Teil einer AWS Organizations Organisation sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
ACM.1	Importierte ACM-issued Zertifikate sollten nach einem	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP	MITTEL	⊘ Ja	Änderung ausgelöst und

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
	bestimmten Zeitraum erneuert werden	800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2			periodisch
ACM.2	Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ACM.3	ACM-Zertifikate sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
Amplify.1	Amplify-Apps sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
Amplify.2	Amplify-Zweige sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	⊙ Ja	Änderung ausgelöst
APIGateway.1	API Gateway, REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway.2	API Gateway, REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
APIGateway.3	Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
APIGateway.4	API Gateway sollte mit einer WAF-Web-ACL verknüpft sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
APIGateway.5	API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway.8	API-Gateway-Routen sollten einen Autorisierungstyp angeben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✓ Ja	Regelmäßig
APIGateway.9	Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
APIGateway.10	API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	✗ Nein	Änderung ausgelöst
APIGateway.11	API-Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
AppConfig.1	AWS AppConfig Anwendungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AppConfig.2	AWS AppConfig Konfigurationsprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
AppConfig.3	AWS AppConfig Umgebungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
AppConfig.4	AWS AppConfig Erweiterungszuordnungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
AppFlow.1	AppFlow Amazon-Datenflüsse sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
AppRunner.1	App Runner-Dienste sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
AppRunner.2	App Runner VPC-Konnektoren sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
AppSync.2	AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AppSync.4	AWS AppSync GraphQL-APIs sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
AppSync.5	AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
Athena.2	Athena-Datenkataloge sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Athena.3	Athena-Arbeitsgruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Athena.4	Athena Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
AutoScaling.1	Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling.2	Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✓ Ja	Änderung ausgelöst
AutoScaling.3	Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
Autoscaling.5	Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
AutoScaling.6	Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling.9	EC2 Auto Scaling Scaling-Gruppen sollten EC2-Startvorlagen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
AutoScaling.10	EC2 Auto Scaling Scaling-Gruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
Backup.1	AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Backup.2	AWS Backup Wiederherstellungspunkte sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
Backup.3	AWS Backup Tresore sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
Backup.4	AWS Backup Berichtspläne sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Backup.5	AWS Backup Backup-Pläne sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Batch.1	Warteschlangen für Batch-Jobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Batch.2	Richtlinien zur Batch-Planung sollten gekennzeichnet sein	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
Batch.3	Batch-Computing-Umgebungen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Batch.4	Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
Bedrock.1	Amazon Bedrock-Datenquellen sollten mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
BedrockAgentCore.1	AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
BedrockAgentCore.2	Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
BedrockAgentCore.3	Bedrock AgentCore Memory sollte mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt werden	NIST SP 800-53 Rev. 5	MITTEL	⊗ Nein	Änderung ausgelöst
BedrockAgentCore.4	Bedrock AgentCore Gateway sollte mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt werden	NIST SP 800-53 Rev. 5	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
BedrockAgentCore.5	AgentCore Benutzerdefinierte Browser von Bedrock sollten den öffentlichen Netzwerkmodus nicht verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
BedrockAgentCore.6	In den AgentCore benutzerdefinierten Browsern von Bedrock sollte die Sitzungsaufzeichnung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
BedrockAgentCore.7	Bedrock-Interpreter für AgentCore benutzerdefinierten Code sollten eine private Netzwerkkonfiguration verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
CloudFormation.2	CloudFormation Stapel sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
CloudFormation.3	CloudFormation Bei Stacks sollte der Kündigungsschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFormation.4	CloudFormation Stacks sollten zugeordnete Servicerollen haben	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.1	CloudFront Bei Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
CloudFront.3	CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.4	CloudFront Bei Distributionen sollte Origin Failover konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront.5	CloudFront Bei Distributionen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.6	CloudFront Bei Distributionen sollte WAF aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.7	CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
CloudFront.8	CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront.9	CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.10	CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CloudFront.12	CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
CloudFront.13	CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront.14	CloudFront Verteilungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
CloudFront.15	CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
CloudFront.16	CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	✗ Nein	Änderung ausgelöst
CloudFront.17	CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail.1	CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, CRI-Profil v2.2 AWS	HIGH (HOCH)	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail.2	CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS CIS Foundations Benchmark v1.4.0 Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
CloudTrail.3	Mindestens ein CloudTrail Trail sollte aktiviert sein	NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail.4	CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, CRI Profile v2.2 AWS	NIEDRIG	⊗ Nein	Regelmäßig
CloudTrail.5	CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail.6	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst und periodisch
CloudTrail.7	Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs für den CloudTrail S3-Bucket aktiviert ist	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, PCI AWS DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudTrail.9	CloudTrail Wege sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
CloudTrail.10	CloudTrail Datenspeicher für Ereignisse in Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	⊙ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.1	Für die Verwendung des Root-Benutzers sollten ein Log-Metrikfilter und ein Alarm vorhanden sein	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.2	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Benchmark für CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.3	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	Benchmark AWS für CIS Foundations v1.2.0, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.4	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.5	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.6	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS-Managementkonsole Authentifizierungsfehler vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.7	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.8	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.9	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.10	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.11	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.12	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.13	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.14	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
CloudWatch.15	CloudWatch Für Alarme sollten bestimmte Aktionen konfiguriert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	HIGH (HOCH)	⊙ Ja	Änderung ausgelöst
CloudWatch.16	CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Regelmäßig
CloudWatch.17	CloudWatch Alarmaktionen sollten aktiviert sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
CodeArtifact.1	CodeArtifact Repositorien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeBuild.1	CodeBuild Die URLs des Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
CodeBuild.2	CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
CodeBuild.3	CodeBuild S3-Protokolle sollten verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
CodeBuild.4	CodeBuild Projektumgebungen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeBuild.7	CodeBuild Exporte von Berichtsgruppen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
CodeGuruProfiler.1	CodeGuru Profiler-Profiling-Gruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	⊙ Ja	Änderung ausgelöst
CodeGuruReviewer.1	CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	⊙ Ja	Änderung ausgelöst
Cognito.1	In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊙ Ja	Änderung ausgelöst
Cognito.2	Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Cognito.3	Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	✓ Ja	Änderung ausgelöst
Cognito.4	In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
Cognito.5	MFA sollte für Cognito-Benutzerpools aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
Cognito.6	In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Config.1	AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, CRI Profile v2.2 AWS	KRITISCH	✓ Ja	Regelmäßig
Connect.1	Die Objekttypen von Connect Customer Profiles sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Connect.2	Connect Customer-Instanzen sollten die CloudWatch Protokollierung aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
DataFirehose.1	Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DataSync.1	DataSync Für Aufgaben sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DataSync.2	DataSync Aufgaben sollten markiert werden	AWS Standard zur Kennzeichnung von Ressourcen, CRI-Profil v2.2	NIEDRIG	⊙ Ja	Änderung ausgelöst
Detective.1	Verhaltensdiagramme von Detektiven sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
DMS.1	Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	KRITISCH	⊗ Nein	Regelmäßig
DMS.2	DMS-Zertifikate sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
DMS.3	DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.4	DMS-Replikationsinstanzen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
DMS.5	Subnetzgruppen für die DMS-Replikation sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
DMS.6	Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversion aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Änderung ausgelöst
DMS.7	Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Änderung ausgelöst
DMS.8	Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.9	DMS-Endpunkte sollten SSL verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DMS.10	Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DMS.11	Auf DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DMS.12	Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.13	DMS-Replikationsinstanzen sollten so konfiguriert sein, dass sie mehrere Availability Zones verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
DocumentDB.1	Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DocumentDB.2	Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
DocumentDB.3	Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DocumentDB.4	Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DocumentDB.5	Für Amazon DocumentDB-Cluster sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DocumentDB.6	Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
DynamoDB.1	DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB 2	In DynamoDB-Tabellen sollte Point-in-Time-Recovery aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
DynamoDB 3	DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
DynamoDB 4	DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Regelmäßig
DynamoDB 5	DynamoDB-Tabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
DynamoDB 6	DynamoDB DynamoDB-Tabellen sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB 7	DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
EC2.1	EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Regelmäßig
EC2.2	VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.3	Angehängte EBS-Volumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EC2.4	Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Regelmäßig
EC2.6	Die VPC-Flussprotokollierung sollte in allen VPCs aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.7	Die EBS-Standardverschlüsselung sollte aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
EC2.8	EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
EC2.9	EC2-Instances sollten keine öffentliche IPv4-Adresse haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.10	Amazon EC2 sollte so konfiguriert sein, dass VPC-Endpunkte verwendet werden, die für den Amazon EC2-Service erstellt wurden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
EC2.12	Ungenutzte EC2-EIPs sollten entfernt werden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
EC2.13	Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst und periodisch
EC2.14	Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389	Benchmark AWS für CIS Foundations v1.2.0, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Ausgelöste und periodische Änderung

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.15	EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EC2.16	Unbenutzte Network Access Control Lists sollten entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
EC2.17	EC2-Instances sollten nicht mehrere ENIs verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
EC2.18	Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	HIGH (HOCH)	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.19	Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst und periodisch
EC2.20	Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EC2.21	Netzwerk-ACLs sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu Port 22 oder Port 3389	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.22	Ungenutzte EC2-Sicherheitsgruppen sollten entfernt werden	CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
EC2.23	EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
EC2.24	Paravirtuelle EC2-Instance-Typen sollten nicht verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EC2.25	EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
EC2.28	EBS-Volumes sollten in einem Backup-Plan enthalten sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊙ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.33	EC2-Transit-Gateway-Anhänge sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.34	Die Routentabellen des EC2-Transit-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.35	EC2-Netzwerkschnittstellen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.36	EC2-Kunden-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.37	EC2-Elastic-IP-Adressen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.38	EC2-Instances sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.39	EC2-Internet-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.40	EC2-NAT-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.41	EC2-Netzwerk-ACLs sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.42	EC2-Routing-Tabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.43	EC2-Sicherheitsgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.44	EC2-Subnetze sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.45	EC2-Volumes sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.46	Amazon VPCs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.47	Amazon VPC Endpoint Services sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.48	Amazon VPC-Flow-Logs sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.49	Amazon VPC-Peering-Verbindungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.50	EC2-VPN-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.51	Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	✗ Nein	Änderung ausgelöst
EC2.52	EC2-Transit-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.53	EC2-Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 zu den Verwaltungsports des Remoteservers	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.54	EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serververwaltungsports zulassen	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
EC2.55	VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	⊙ Ja	Regelmäßig
EC2.56	VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	⊙ Ja	Regelmäßig
EC2.57	VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	⊙ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.58	VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	✓ Ja	Regelmäßig
EC2.60	VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	✓ Ja	Regelmäßig
EC2.170	EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	NIEDRIG	✗ Nein	Änderung ausgelöst
EC2.171	Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.172	Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✓ Ja	Änderung ausgelöst
EC2.173	EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
EC2.174	EC2-DHCP-Optionssätze sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.175	EC2-Startvorlagen sollten mit Tags versehen sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.176	EC2-Präfixlisten sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.177	EC2-Traffic-Mirror-Sitzungen sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.178	EC2-Traffic-Spiegelfilter sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.179	EC2-Traffic-Mirror-Ziele sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EC2.180	Bei EC2-Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
EC2.181	EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
EC2.182	EBS-Snapshots sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
EC2.183	EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
ECR.1	Für private ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECR.2	Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ECR.3	Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ECR.4	Öffentliche ECR-Repositorien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
ECR.5	Die ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	⊙ Ja	Änderung ausgelöst
ECS.2	ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.3	ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ECS.4	ECS-Container sollten ohne Zugriffsrechte ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ECS.5	ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ECS.8	Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.9	ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ECS.10	ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ECS.12	ECS-Cluster sollten Container Insights verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ECS.13	ECS-Dienste sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
ECS.14	ECS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.15	ECS-Aufgabendefinitionen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
ECS.16	ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
ECS.17	ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
ECS.18	ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
ECS.19	ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.20	ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Containerdefinitionen konfigurieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
ECS.21	ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
EFS.1	Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
EFS.2	Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS.3	EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EFS.4	EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EFS.5	EFS-Zugangspunkte sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
EFS.6	EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
EFS.7	EFS EFS-Dateisystemen sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS.8	EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden	CIS AWS Foundations Benchmark v5.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, CRI-Profil v2.2	MITTEL	✓ Ja	Änderung ausgelöst
EKS.1	EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig
EKS.2	EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Änderung ausgelöst
EKS.6	EKS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
EKS.7	Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EKS.8	Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EKS.9	EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
ElastiCache.1	ElastiCache Bei Clustern (Redis OSS) sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	✓ Ja	Regelmäßig
ElastiCache.2	ElastiCache Bei Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElastiCache.3	ElastiCache Für Replikationsgruppen sollte der automatische Failover aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
ElastiCache.4	ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
ElastiCache.5	ElastiCache Replikationsgruppen sollten während der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
ElastiCache.6	ElastiCache (Redis OSS) Für Replikationsgruppen früherer Versionen sollte Redis OSS AUTH aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElastiCache.7	ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
ElasticBeanstalk.1	In Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
ElasticBeanstalk.2	Von Elastic Beanstalk verwaltete Plattform updates sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊙ Ja	Änderung ausgelöst
ElasticBeanstalk.3	Elastic Beanstalk sollte Logs streamen nach CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.1	Der Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
ELB.2	Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.3	Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.4	Der Application Load Balancer sollte so konfiguriert sein, dass er HTTP-Header löscht	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.5	Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.6	Für Anwendung, Gateway und Network Load Balancer sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.7	Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
ELB.8	Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Konfiguration verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.9	Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.10	Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
ELB.12	Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.13	Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.14	Der Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.16	Application Load Balancers sollten mit einer AWS WAF-Web-ACL verknüpft sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.17	Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.18	Applications- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.21	Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ELB.22	ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EMR.1	Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
EMR.2	Die Einstellung „Öffentlichen Zugriff blockieren“ in Amazon EMR sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EMR.3	Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
EMR.4	Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.1	Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
ES.2	Elasticsearch-Domains sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.3	Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.4	Die Protokollierung von Elasticsearch-Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.5	Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.6	Elasticsearch-Domains sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.7	Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.8	Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
ES.9	Elasticsearch-Domains sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
EventBridge.2	EventBridge Eventbusse sollten markiert sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
EventBridge.3	EventBridge An benutzerdefinierte Event-Busse sollte eine ressourcenbasierte Richtlinie angehängt sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EventBridge.4	EventBridge Auf globalen Endpunkten sollte die Ereignisreplikation aktiviert sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
FraudDetector.1	Die Entitätstypen von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
FraudDetector.2	Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
FraudDetector.3	Die Ergebnisse von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
FraudDetector.4	Die Variablen von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
FSx.1	FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
FSx.2	FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
FSx.3	FSx für OpenZFS-Dateisysteme sollten für die Bereitstellung konfiguriert werden Multi-AZ	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
FSx.4	FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊘ Ja	Regelmäßig
FSx.5	FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
Glue.1	AWS Glue Jobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊘ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Glue.3	AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Glue.4	AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
GlobalAccelerator.1	Global Accelerator-Beschleuniger sollten markiert sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
GuardDuty.1	GuardDuty sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
GuardDuty.2	GuardDuty Filter sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
GuardDuty.3	GuardDuty IPSets sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
GuardDuty.4	GuardDuty Melder sollten markiert sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
GuardDuty.5	GuardDuty EKS Audit Log Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig
GuardDuty.6	GuardDuty Lambda-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig
GuardDuty.7	GuardDuty EKS Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig
GuardDuty.8	GuardDuty Der Malware-Schutz für EC2 sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
GuardDuty.9	GuardDuty RDS-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
GuardDuty.10	GuardDuty S3-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
GuardDuty.11	GuardDuty Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
GuardDuty.12	GuardDuty ECS Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
GuardDuty.13	GuardDuty EC2 Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.1	IAM-Richtlinien sollten keine vollen „*“ - Administratorrechte zulassen	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
IAM.2	IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.3	Die Zugangsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2 AWS	MITTEL	⊗ Nein	Regelmäßig
IAM.4	Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2 AWS	KRITISCH	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.5	MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2 AWS	MITTEL	⊗ Nein	Regelmäßig
IAM.6	Hardware-MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2 AWS	KRITISCH	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.7	Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	Ja	Regelmäßig
IAM.8	Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.9	MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2 AWS	KRITISCH	⊗ Nein	Regelmäßig
IAM.10	Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben	NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.11	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Benchmark für CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.12	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Benchmark für CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.13	Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Benchmark für CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.14	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	Benchmark für CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.15	Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2 AWS	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.16	Sicherstellen, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2 AWS	NIEDRIG	⊗ Nein	Regelmäßig
IAM.17	Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Benchmark AWS für CIS Foundations v1.2.0, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.18	Stellen Sie sicher, dass eine Support-Rolle für die Bearbeitung von Vorfällen eingerichtet wurde AWS Support	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2 AWS	NIEDRIG	⊗ Nein	Regelmäßig
IAM.19	MFA sollte für alle IAM-Benutzer aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.21	Von Ihnen erstellte, vom Kunden verwaltete IAM-Richtlinien sollten keine Platzhalteraktionen für Dienste zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.22	IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.23	IAM Access Analyzer-Analyzer sollten markiert sein	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
IAM.24	IAM-Rollen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
IAM.25	IAM-Benutzer sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
IAM.26	Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
IAM.27	IAM-Identitäten sollte die Richtlinie nicht beigefügt sein AWSCloudShellFullAccess	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.28	Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
Inspector.1	Amazon Inspector EC2-Scannen sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
Inspector.2	Das Amazon Inspector ECR-Scannen sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
Inspector.3	Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
Inspector.4	Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoT.1	AWS IoT Device Defender Sicherheitsprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoT.2	AWS IoT Core Maßnahmen zur Schadensbegrenzung sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoT.3	AWS IoT Core Dimensionen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoT.4	AWS IoT Core Autorisierer sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoT.5	AWS IoT Core Rollenaliase sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoT.6	AWS IoT Core Richtlinien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTSiteWise.1	AWS IoT SiteWise Asset-Modelle sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoTSiteWise.2	AWS IoT SiteWise Dashboards sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTSiteWise.3	AWS IoT SiteWise Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTSiteWise.4	AWS IoT SiteWise Portale sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTSiteWise.5	AWS IoT SiteWise Projekte sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTTwinMaker.1	AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTTwinMaker.2	AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTTwinMaker.3	AWS TwinMaker IoT-Szenen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoTTwinMaker.4	AWS TwinMaker IoT-Entitäten sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTWireless.1	AWS IoT-Wireless-Multicast-Gruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTWireless.2	AWS IoT-Wireless-Dienstprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IoTWireless.3	AWS IoT Wireless FUOTA-Aufgaben sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
IVS.1	Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
IVS.2	IVS-Aufnahmekonfigurationen sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
IVS.3	IVS-Kanäle sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Keyspaces.1	Amazon Keyspaces-Keyspaces sollten markiert werden	AWS Standard für Ressourcen-Tagging, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
Kinesis.1	Kinesis-Streams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
Kinesis.2	Kinesis-Streams sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
Kinesis.3	Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✓ Ja	Änderung ausgelöst
KMS.1	Vom Kunden verwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
KMS.2	IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
KMS.3	AWS KMS keys sollte nicht ungewollt gelöscht werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
KMS.4	AWS KMS key Rotation sollte aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2 AWS	MITTEL	⊗ Nein	Regelmäßig
KMS.5	KMS-Schlüssel sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.1	Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
Lambda.2	Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Lambda.3	Lambda-Funktionen sollten sich in einer VPC befinden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
Lambda.5	VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
Lambda.6	Lambda-Funktionen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.7	Lambda Lambda-Funktionen sollte die AWS X-Ray aktive Ablaufverfolgung aktiviert sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
Macie.1	Amazon Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
Macie.2	Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
MSK.1	MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
MSK.2	Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
MSK.3	MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
MSK.4	Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
MSK.5	Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
MSK.6	MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
MQ.2	ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
MQ.4	Amazon MQ-Broker sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
MQ.5	ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
MQ.6	RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
Neptune.1	Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Neptune.2	Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Neptune.3	Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptune.4	Neptune Neptune-DB-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
Neptune.5	Neptune Neptune-DB-Clustern sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
Neptune.6	Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Neptune.7	Neptune Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptune.8	Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
Neptune.9	Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
NetworkFirewall.1	Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
NetworkFirewall.2	Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall.3	Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
NetworkFirewall.4	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
NetworkFirewall.5	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
NetworkFirewall.6	Die Regelgruppe für statuslose Netzwerk-Firewalls sollte nicht leer sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall.7	Netzwerk-Firewall-Firewalls sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
NetworkFirewall.8	Netzwerk-Firewall-Firewall-Richtlinien sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
NetworkFirewall.9	Network Firewall Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
NetworkFirewall.10	Network Firewall Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
Opensearch.1	OpenSearch Bei Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Opensearch.2	OpenSearch Domains sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
Opensearch.3	OpenSearch Domänen sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Opensearch.4	OpenSearch Die Protokollierung von Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Opensearch.5	OpenSearch Für Domänen sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Opensearch.6	OpenSearch Domänen sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Opensearch.7	OpenSearch Für Domänen sollte eine fein abgestufte Zugriffskontrolle aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
Opensearch.8	Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Opensearch.9	OpenSearch Domains sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
Opensearch.10	OpenSearch In den Domänen sollte das neueste Softwareupdate installiert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Opensearch.11	OpenSearch Domänen sollten mindestens drei dedizierte Primärknoten haben	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
PCA.1	AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
PCA.2	AWS Private Zertifizierungsstellen sollten gekennzeichnet werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
RDS.1	Der RDS-Snapshot sollte privat sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.2	RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
RDS.3	Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.4	RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.5	RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden	CIS AWS Foundations Benchmark v5.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.6	Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
RDS.7	Bei RDS-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.8	Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.9	RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.10	Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.11	Für RDS-Instances sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
RDS.12	Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.13	Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
RDS.14	Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
RDS.15	RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden	CIS AWS Foundations Benchmark v5.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.16	Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.17	RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.19	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.20	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.21	Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.22	Für kritische Ereignisse in Datenbanksicherheitsgruppen sollte ein Abonnement für RDS-Ereignisbenachrichtigungen konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.23	RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.24	RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.25	RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.26	RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Regelmäßig
RDS.27	RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.28	RDS-DB-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
RDS.29	RDS-DB-Cluster-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
RDS.30	RDS-DB-Instances sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.31	RDS-DB-Sicherheitsgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
RDS.32	RDS-DB-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
RDS.33	RDS-DB-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
RDS.34	Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
RDS.35	Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Änderung ausgelöst
RDS.36	RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.37	Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
RDS.38	RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
RDS.39	RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
RDS.40	RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	✓ Ja	Änderung ausgelöst
RDS.41	RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
RDS.42	RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	✓ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.43	RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Regelmäßig
RDS.44	RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
RDS.45	Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
RDS.46	RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Regelmäßig
RDS.47	RDS für PostgreSQL-DB-Cluster sollten so konfiguriert werden, dass Tags in DB-Snapshots kopiert werden	AWS Bewährte grundlegende Sicherheitsmethoden	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.48	RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden	AWS Bewährte grundlegende Sicherheitsmethoden	NIEDRIG	⊗ Nein	Änderung ausgelöst
RDS.50	Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Ja	Änderung ausgelöst
RDS.51	Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
Redshift.1	Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.2	Verbindungen zu Amazon Redshift Redshift-Clustern sollten während der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Redshift.3	Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
Redshift.4	Amazon Redshift Redshift-Cluster sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Redshift.6	Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.7	Redshift-Cluster sollten erweitertes VPC-Routing verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Redshift.8	Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Redshift.10	Redshift-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
Redshift.11	Redshift-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst
Redshift.12	Abonnementbenachrichtigungen für Redshift-Ereignisse sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.13	Redshift-Cluster-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
Redshift.14	Redshift-Cluster-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
Redshift.15	Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Ursprüngen zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	✗ Nein	Regelmäßig
Redshift.16	Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
Redshift.17	Redshift-Cluster-Parametergruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
Redshift.18	Redshift Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RedshiftServerless.1	Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
RedshiftServerless.2	Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
RedshiftServerless.3	Redshift Serverlose Arbeitsgruppen sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
RedshiftServerless.4	Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	✓ Ja	Regelmäßig
RedshiftServerless.5	Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RedshiftServerless.6	Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
Route53.1	Gesundheitschecks auf Route 53 sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
Route53.2	In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
S3.1	Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.2	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst und periodisch
S3.3	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Schreibzugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst und periodisch
S3.5	Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erforderlich sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.6	Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
S3.7	S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
S3.8	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Zugriff blockieren	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.9	Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
S3.10	S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
S3.11	Für S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊘ Ja	Änderung ausgelöst
S3.12	ACLs sollten nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
S3.13	S3-Buckets für allgemeine Zwecke sollten Lifecycle-Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊘ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.14	Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst
S3.15	Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊘ Ja	Änderung ausgelöst
S3.17	S3-Buckets für allgemeine Zwecke sollten im Ruhezustand mit verschlüsselt werden AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
S3.19	Bei S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	KRITISCH	⊗ Nein	Änderung ausgelöst
S3.20	Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.22	S3-Buckets für allgemeine Zwecke sollten Schreiberignisse auf Objektebene protokollieren	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
S3.23	S3-Buckets für allgemeine Zwecke sollten Leseereignisse auf Objektebene protokollieren	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
S3.24	Für S3 Multi-Region Access Points sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
S3.25	S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.1	Amazon SageMaker Notebook-Instances sollten keinen direkten Internetzugang haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Regelmäßig
SageMaker.2	SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
SageMaker.3	Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instanzen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
SageMaker.4	SageMaker Bei Produktionsvarianten für Endgeräte sollte die anfängliche Anzahl der Instanzen größer als 1 sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.5	SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.6	SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
SageMaker.7	SageMaker Bilder sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
SageMaker.8	SageMaker Notebook-Instanzen sollten auf unterstützten Plattformen laufen	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Regelmäßig
SageMaker.9	SageMaker Für Auftragsdefinitionen zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.10	SageMaker Bei den Auftragsdefinitionen zur Erläuterung des Modells sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.11	SageMaker Für Auftragsdefinitionen zur Datenqualität sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.12	SageMaker Bei Jobdefinitionen mit Modellverzerrung sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.13	SageMaker Für Auftragsdefinitionen in Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.14	SageMaker In den Überwachungszeitplänen sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.15	SageMaker Bei den Jobdefinitionen mit Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.16	SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.17	SageMaker Offline-Stores für Featuregruppen sollten mit AWS KMS Schlüsseln verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.18	SageMaker Onlineshops für Featuregruppen mit Standardspeicher sollten mit AWS KMS Schlüsseln verschlüsselt werden	NIST SP 800-53 Rev. 5	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.19	SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.20	SageMaker Bei Auftragsdefinitionen zur Erläuterung des Modells sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
SageMaker.21	SageMaker Notebook-Instanzen sollten mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker.22	SageMaker In den Überwachungszeitplänen sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.23	SageMaker Bei Inferenzexperimenten sollte das Instanz-Speichervolumen mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.24	SageMaker Bei Inferenzexperimenten sollte der Datenspeicher mit vom Kunden verwalteten AWS KMS Schlüsseln verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	⊗ Nein	Änderung ausgelöst
SageMaker.25	SageMaker Bei Auftragsdefinitionen für Modellqualität sollte die Netzwerkisolierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SecretsManager.1	Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✓ Ja	Änderung ausgelöst
SecretsManager.2	Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Änderung ausgelöst
SecretsManager.3	Unbenutzte Secrets Manager Manager-Geheimnisse entfernen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✓ Ja	Regelmäßig
SecretsManager.4	Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✓ Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SecretsManager.5	Secrets Manager Manager-Geheimnisse sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
ServiceCatalog.1	Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Regelmäßig
SES.1	SES-Kontaktlisten sollten mit Tags versehen sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
SES.2	SES-Konfigurationssätze sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
SES.3	In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	✗ Nein	Änderung ausgelöst
SNS.1	SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SNS.3	SNS-Themen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
SNS.4	Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	KRITISCH	✗ Nein	Änderung ausgelöst
SQS.1	Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
SQS.2	SQS-Warteschlangen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	✓ Ja	Änderung ausgelöst
SQS.3	Die SQS-Richtlinien für den Warteschlangenzugriff sollten keinen öffentlichen Zugriff zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, CRI-Profil v2.2	KRITISCH	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM.1	EC2-Instances sollten verwaltet werden von AWS Systems Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
SSM.2	Von Systems Manager verwaltete EC2-Instances sollten nach einer Patch-Installation den Patch-Konformitätsstatus COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (HOCH)	⊗ Nein	Änderung ausgelöst
SSM.3	Von Systems Manager verwaltete EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	NIEDRIG	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM.4	SSM-Dokumente sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	KRITISCH	⊗ Nein	Regelmäßig
SSM.5	SSM-Dokumente sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst
SSM.6	Bei SSM Automation sollte die CloudWatch Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	MITTEL	⊗ Nein	Regelmäßig
SSM.7	Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, CRI-Profil v2.2	KRITISCH	⊗ Nein	Regelmäßig
StepFunctions.1	Step Functions, bei Zustandsmaschinen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	⊙ Ja	Änderung ausgelöst
StepFunctions.2	Step Functions Functions-Aktivitäten sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	⊙ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Transfer.1	Die Workflows von Transfer Family sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Transfer.2	Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MITTEL	✗ Nein	Regelmäßig
Transfer.3	Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
Transfer.4	Transfer Family Familienverträge sollten gekennzeichnet werden	AWS Standard zur Kennzeichnung von Ressourcen, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst
Transfer.5	Transfer Family Familienzertifikate sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
Transfer.6	Steckverbinder der Transfer-Familie sollten gekennzeichnet sein	AWS Standard zur Kennzeichnung von Ressourcen, CRI-Profil v2.2	NIEDRIG	✓ Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Transfer.7	Transfer Family Familienprofile sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	✓ Ja	Änderung ausgelöst
WAF.1	AWS Die WAF Classic Global Web ACL-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	MITTEL	✗ Nein	Regelmäßig
WAF.2	AWS Die regionalen Regeln von WAF Classic sollten mindestens eine Bedingung enthalten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst
WAF.3	AWS WAF Classic Regional Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	✗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.4	AWS WAF Classic Regional Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WAF.6	AWS Globale WAF Classic-Regeln sollten mindestens eine Bedingung haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WAF.7	AWS Globale WAF Classic-Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WAF.8	AWS Globale WAF Classic-Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.10	AWS WAF-Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WAF.11	AWS Die WAF-Web-ACL-Protokollierung sollte aktiviert sein	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI-Profil v2.2	NIEDRIG	⊗ Nein	Regelmäßig
WAF.12	AWS Bei WAF-Regeln sollten CloudWatch Metriken aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI-Profil v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WorkSpaces.1	WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst
WorkSpaces.2	WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, CRI Profile v2.2	MITTEL	⊗ Nein	Änderung ausgelöst

Änderungsprotokoll für Security Hub CSPM-Steuerelemente

Das folgende Änderungsprotokoll verfolgt wesentliche Änderungen an bestehenden AWS Security Hub CSPM-Kontrollen, die zu Änderungen des Gesamtstatus einer Kontrolle und des Compliance-Status ihrer Ergebnisse führen können. Informationen darüber, wie Security Hub CSPM den Kontrollstatus bewertet, finden Sie unter. Bewertung des Konformitätsstatus und des Kontrollstatus Es kann einige Tage nach ihrem Eintrag in diesem Protokoll dauern, bis sich Änderungen auf alle auswirken, AWS-Regionen in denen das Steuerelement verfügbar ist.

In diesem Protokoll werden Änderungen aufgezeichnet, die seit April 2023 vorgenommen wurden. Wählen Sie ein Steuerelement aus, um weitere Details dazu zu überprüfen. Titeländerungen werden 90 Tage lang in der detaillierten Beschreibung eines Steuerelements vermerkt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. Oktober 2026	[Bedrock.1] Amazon Bedrock-Datenquellen sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	Security Hub CSPM hat die Steuerung aktualisiert, sodass Datenquellen, die zu einer verwalteten Wissensdatenbank gehören, nicht ausgewertet werden, da die serverseitige Verschlüsselung für eine verwaltete Wissensdatenbank in der Wissensda tenbank und nicht in ihren Datenquellen konfiguriert ist.
23. September 2026	[BedrockAgentCore.1] AgentCore Bedrock-L aufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden	Security Hub CSPM hat die Steuerung aktualisiert, sodass Laufzeiten, die von einem Kapazität

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		sanbieter unterstützt werden, nicht ausgewertet werden, da solche Laufzeiten ihre Netzwerkkonfiguration auf dem Kapazitätsanbieter und nicht auf der Laufzeit definieren.
11. September 2026	[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein	Dieses Steuerelement prüft, ob das automatische Upgrade einer Nebenversion für einen Amazon RDS-DB-Cluster aktiviert ist. Security Hub CSPM erweiterte die Kontrolle auf die Evaluierung von Aurora-DB-Clustern, die zuvor keine Ergebnisse lieferten.
11. September 2026	[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein	Security Hub CSPM hat den Titel und die Beschreibung dieses Steuerelements aktualisiert und bezieht sich nun auf TLS statt auf SSL, da SSL veraltet ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. August 2026	[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten	Diese Kontrolle prüft, ob Amazon RDS-Instances den öffentlichen Zugriff verbieten. Da Neptune DB jetzt öffentliche Endpunkte unterstützt, bewertet und generiert diese Steuerung umsetzbare Ergebnisse für Neptune DB-Instances. Security Hub CSPM hat die Beschreibung der Steuerung aktualisiert, um dieser Änderung Rechnung zu tragen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. August 2026	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `1.33` auf geändert. `1.34` Die Standardunterstützung für Kubernetes Version 1.33 in Amazon EKS endete am 29. Juli 2026.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. August 2026	[EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob eine Amazon EKS-Knotengruppe auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `1.33` auf geändert. `1.34` Die Standardunterstützung für Kubernetes Version 1.33 in Amazon EKS endete am 29. Juli 2026.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
3. August 2026	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `java17.al2023`, `java11.al2023`, `java8.al2023` als Parameterwert, ebenso wie Unterstützung für diese Laufzeit hinzugefügt AWS Lambda wurde.
3. August 2026	[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen	Security Hub CSPM hat diese Kontrolle aus dem Standard AWS Foundational Security Best Practices (FSBP) entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Juli 2026	[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen	Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `notebook-al2-v3` auf geändert. `notebook-al2023-v1` SageMaker AI hat Notebook-Instance-Plattformen von Amazon Linux 2 auf AL2023 migriert.
13. Juli 2026	[EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden	Security Hub CSPM hat die Backing-Regel für dieses Steuerelement von service-vpc-endpoint-enabled auf vpc-endpoint-enabled geändert. Die aktualisierte Regel erkennt die Namen der FIPS-variant Endpunktdienste als konform an und generiert einen Befund für VPCs, die FIPS-Endpunkte verwenden. `PASSED`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. Juni 2026	[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen	Security Hub CSPM hat diese Steuerung zu den folgenden geltenden Standards hinzugefügt — dem Standard NIST SP 800-53 Rev. 5, dem Standard NIST SP 800-171 Revision2 und dem Standard PCI DSS v4.0.1. Am 30. Juli 2026 wird dieses Steuerelement aus dem FSBP-Standard (Foundational Security Best Practices) entfernt. AWS

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Juni 2026	[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden	Security Hub CSPM hat mitgeteilt, dass diese Kontrolle nach dem 10. August 2026 eingestellt und aus allen geltenden Security Hub CSPM-Standards entfernt wird. Ab Kubernetes-Version 1.28 verfügen Amazon EKS-Clust er standardmäßig über Kubernetes-Geheimnisse, die mit Umschlagverschlüss elung geschützt sind.
5. Juni 2026	[IoTEvents.1] AWS IoT-Events-Eingaben sollten markiert werden	Security Hub CSPM hat mitgeteilt, dass diese Kontrolle nach dem 7. Juli 2026 eingestellt und aus allen geltenden Security Hub CSPM-Standards entfernt wird. AWS kündigte das Ende des Supports für den AWS IoT Events Events-Se rvice mit Wirkung zum 20. Mai 2026 an.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Juni 2026	[IoTEvents.2] Modelle mit AWS IoT-Ereignisdetektoren sollten markiert werden	Security Hub CSPM hat mitgeteilt, dass diese Kontrolle nach dem 7. Juli 2026 eingestellt und aus allen geltenden Security Hub CSPM-Standards entfernt wird. AWS kündigte das Ende des Supports für den AWS IoT Events Events-Service mit Wirkung zum 20. Mai 2026 an.
5. Juni 2026	[IoTEvents.3] Alarmmodelle für AWS IoT Events sollten markiert werden	Security Hub CSPM hat mitgeteilt, dass diese Kontrolle nach dem 7. Juli 2026 eingestellt und aus allen geltenden Security Hub CSPM-Standards entfernt wird. AWS kündigte das Ende des Supports für den AWS IoT Events Events-Service mit Wirkung zum 20. Mai 2026 an.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Juni 2026	[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten	Security Hub CSPM hat diese Kontrolle zurückgezogen und sie aus allen geltenden Standards entfernt. Zuvor prüfte die Steuerung, ob eine aktive Amazon ECS-Aufgabendefinition, die den Host-Netzwerkmodus verwendete, auch `user` Container-Definitionen hatte`privileged` .

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Juni 2026	[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden	Security Hub CSPM hat diese Kontrolle zurückgezogen und sie aus allen geltenden Standards entfernt. Seit der Einstellung von Amazon EC2-Classic Networking können Amazon Relational Database Service (Amazon RDS) -Instances nicht mehr außerhalb einer VPC bereitgestellt werden. Zuvor prüfte die Steuerung, ob eine Amazon RDS-Instance auf einem bereitgestellt wurde EC2-VPC.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
4. Mai 2026	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt diese Laufzeit jetzt `ruby4.0` als Parameter und schließt diese Laufzeit nicht mehr ein, `nodejs20.x` da sie veraltet AWS Lambda ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. April 2026	[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden	Security Hub CSPM hat die unterstützende Regel für dieses Steuerelement von ec2-stopped-instance in eine benutzerdefinierte Security Hub-CSPM-Regel, ec2-stopped-instance-days-check, geändert, um die Bewertungslogik zu vereinfachen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. April 2026	[EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind	Security Hub CSPM hat den Titel und die Beschreibung dieses Steuerelements geändert. Der neue Titel und die neue Beschreibung geben genauer wieder, dass das Steuerelement prüft, ob Amazon EBS-Snapshots so konfiguriert sind, dass sie öffentlich wiederherstellbar sind. Bisher lautete der Titel dieses Steuerelements: Amazon EBS-Snaps hots sollten nicht öffentlich wiederher stellbar sein.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. April 2026	[EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein	Security Hub CSPM hat den Titel und die Beschreibung dieses Steuerelements geändert. Der neue Titel und die neue Beschreibung geben genauer wieder, dass die Steuerung prüft, ob die Sperrung des öffentlichen Zugriffs auf Kontoebene für Amazon EBS-Snapshots aktiviert ist. Bisher lautete der Titel dieses Steuerelements: Amazon EBS-Snapshots sollten nicht öffentlich zugänglich sein.
6. April 2026	[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden	Security Hub CSPM hat den Parameterwert für dieses Steuerelement aktualisiert, um die empfohlenen Sicherheitsrichtlinien widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
3. April 2026	[Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben	Security Hub CSPM erweiterte den Bereich der unterstützten Werte für den `temporaryPasswordValidity` Parameter dieses Steuerelements. Sie können jetzt einen Wert zwischen 1 und 365 Tagen angeben. Zuvor lag der Bereich zwischen 7 und 365 Tagen.
3. April 2026	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `1.32` auf `1.33` geändert. Die Standardunterstützung für Kubernetes Version 1.32 in Amazon EKS endete am 23. März 2026.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
3. April 2026	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 Der Parameter für unterstützte Laufzeiten ist nicht mehr enthalten, `ruby3.2` da Lambda diese Laufzeit als veraltet eingestuft hat.
24. März 2026	[RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein	Security Hub CSPM hat den Titel des Steuerelements aktualisiert, um widerzuspiegeln, dass das Steuerelement alle RDS-DB-Cluster überprüft.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
24. März 2026	[ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind	Security Hub CSPM hat den Titel und die Beschreibung des Steuerelements aktualisiert, um zu verdeutlichen, dass das Steuerelement die ECS-Aufgabendefinitionen überprüft. Security Hub CSPM hat außerdem die Steuerung aktualisiert, sodass keine Ergebnisse für Aufgabendefinitionen generiert werden, die für die Angabe einer `WINDOWS_SERVER` Betriebssystemfamilie `runtimePlatform` konfiguriert sind.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
9. März 2026	[AppSync.1] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden	Security Hub CSPM hat dieses Steuerelement zurückgezogen und es aus dem FSBP-Standard (AWS Foundational Security Best Practices) entfernt. AWS AppSync bietet jetzt Standardverschlüsselung für alle aktuellen und future API-Caches.
9. März 2026	[AppSync.6] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden	Security Hub CSPM hat dieses Steuerelement zurückgezogen und es aus dem FSBP-Standard (AWS Foundational Security Best Practices) entfernt. AWS AppSync bietet jetzt Standardverschlüsselung für alle aktuellen und future API-Caches.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
4. März 2026	[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten	Security Hub CSPM hat dieses Steuerelement zurückgezogen und es aus dem Standard AWS Foundational Security Best Practices (FSBP) und dem Standard NIST SP 800-53 Rev. 5 entfernt.
5. Februar 2026	[AppSync.1] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden	Security Hub CSPM wird diese Kontrolle abschaffen und am 9. März 2026 aus allen geltenden Security Hub CSPM-Standards streichen. AWS AppSync bietet Standardverschlüsselung für alle aktuellen und future API-Caches.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Februar 2026	[AppSync.6] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden	Security Hub CSPM wird diese Kontrolle abschaffen und am 9. März 2026 aus allen geltenden Security Hub CSPM-Standards streichen . AWS AppSync bietet Standardv erschlüsselung für alle aktuellen und future API-Caches.
16. Januar 2026	[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerd efinitionen enthalten	Security Hub CSPM hat mitgeteilt, dass diese Kontrolle nach dem 16. Februar 2026 eingestellt und aus allen geltenden Security Hub CSPM-Standards entfernt wird.
12. Januar 2026	[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein	Security Hub CSPM hat dieses Steuerele ment aktualisiert, um den `loggingEn abled` Parameter zu entfernen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. Januar 2026	[MQ.3] Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben	Security Hub CSPM hat die Kontrolle zurückgezogen und die Kontrolle aus allen geltenden Standards entfernt. Security Hub CSPM hat die Kontrolle aufgrund der Amazon MQ MQ-Anforderungen für automatische Upgrades kleinerer Versionen eingestellt. Bisher galt die Kontrolle für den Standard AWS Foundational Security Best Practices (FSBP), den StandardNIST SP 800-53 Rev. 5 und den Standard PCI DSS v4.0.1.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. Januar 2026	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement jetzt `dotnet10` als Parameterwert. AWS Lambda Unterstützung für diese Runtime hinzugefügt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. Dezember 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement nicht mehr `python3.9` als Parameterwert. AWS Lambda unterstützt diese Laufzeit nicht mehr.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. Dezember 2025	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `1.31` auf geändert. `1.32` Die Standardunterstützung für Kubernetes Version 1.31 in Amazon EKS endete am 26. November 2025.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
21. November 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt jetzt `nodejs24.x` und `python3.14` als Parameterwerte für dieses Steuerelement. AWS Lambda Unterstützung für diese Laufzeiten hinzugefügt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. November 2025	[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	Security Hub CSPM hat die Beschreibung und Begründung für diese Kontrolle aktualisiert. Bisher überprüfte das Steuerelement mithilfe des Flags nur die automatische Zuweisung von öffentlichen IPv4-IP-Adressen in Amazon VPC-Subnetzen. `MapPublicIpOnLaunch` Dieses Steuerelement prüft jetzt sowohl die automatische Zuweisung von öffentlichen IPv4- als auch IPv6-IP-Adressen. Die Beschreibung und Begründung des Steuerelements wurden aktualisiert, um diesen Änderungen Rechnung zu tragen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. November 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement jetzt `java25` als Parameterwert. AWS Lambda Unterstützung für diese Runtime hinzugefügt.
13. November 2025	[SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `HIGH` auf geändert. `CRITICAL` Der öffentliche Zugriff auf Amazon SNS SNS-Themen stellt ein erhebliches Sicherheitsrisiko dar.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. November 2025	[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `HIGH` auf geändert. `CRITICAL` Der öffentliche Zugriff auf Amazon SQS SQS-Warteschlangen stellt ein erhebliches Sicherheitsrisiko dar.
13. November 2025	[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `MEDIUM` auf geändert. `HIGH` Diese Art der Laufzeitüberwachung bietet eine verbesserte Bedrohungserkennung für Amazon EKS-Ressourcen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. November 2025	[MQ.3] Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `LOW` auf geändert. `MEDIUM` Kleinere Versions-Upgrades beinhalten Sicherheitspatches, die für die Aufrechterhaltung der Amazon MQ-Broker-Sicherheit erforderlich sind.
13. November 2025	Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `LOW` auf geändert. `MEDIUM` Softwareupdates enthalten Sicherheitspatches, die für die Aufrechterhaltung der OpenSearch Domänensicherheit erforderlich sind.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. November 2025	[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `LOW` auf geändert. `MEDIUM` Der Löschschutz trägt dazu bei, das versehentliche Löschen von Amazon RDS-Datenbanken und das Löschen von RDS-Datenbanken durch nicht autorisierte Entitäten zu verhindern.
13. November 2025	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `LOW` auf geändert. `MEDIUM` AWS CloudTrail Die Protokollierung von Daten in Amazon CloudWatch Logs kann für Prüfaktivitäten, Alarme und andere wichtige Sicherheitsoperationen verwendet werden.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. November 2025	[ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `HIGH` auf geändert. `MEDIUM` Das Teilen von AWS Service Catalog Portfolios mit bestimmten Konten kann beabsichtigt sein und bedeutet nicht unbedingt, dass ein Portfolio öffentlich zugänglich ist.
13. November 2025	[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `MEDIUM` auf geändert. `LOW` `cloudfron t.net` Standard-Domainnamen für CloudFront Amazon-Distributio nen werden nach dem Zufallsprinzip generiert, wodurch das Sicherheitsrisiko reduziert wird.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. November 2025	[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein	Security Hub CSPM hat den Schweregrad dieser Kontrolle von `MEDIUM` auf geändert. `LOW` In Bereitstellungen mit mehreren Instanzen können andere fehlerfreie Instances Benutzersitzungen verarbeiten, wenn eine Instanz beendet wird, ohne dass die Verbindung unterbrochen wird. Dadurch werden betriebliche Auswirkungen und Verfügbarkeitsrisiken reduziert.
13. November 2025	[RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden	Security Hub CSPM hat dieses Steuerelement aktualisiert, um den optionalen `validAdminUserNames` Parameter zu entfernen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
23. Oktober 2025	Bei [ElastiCache.1] ElastiCache (Redis OSS) - Clustern sollten automatische Backups aktiviert sein	Security Hub CSPM hat die Änderungen, die am 14. Oktober 2025 am Titel, der Beschreibung und der Regel für diese Kontrolle vorgenommen wurden, rückgängig gemacht.
22. Oktober 2025	Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	Security Hub CSPM hat diese Steuerung aktualisiert, sodass keine Ergebnisse für CloudFront Amazon-Distributionen generiert werden, die benutzerdefinierte Ursprünge verwenden.
16. Oktober 2025	[CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden	Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution für die Verwendung einer empfohlenen TLS-Sicherheitsrichtlinie konfiguriert ist. Security Hub CSPM unterstützt jetzt `TLSv1.2_2025` und `TLSv1.3_2025` als Parameterwerte für dieses Steuerelement.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. Oktober 2025	Bei [ElastiCache.1] ElastiCache (Redis OSS) - Clustern sollten automatische Backups aktiviert sein	Security Hub CSPM hat den Titel, die Beschreibung und die Regel für dieses Steuerelement geändert. Zuvor überprüfte das Steuerelement Redis OSS-Cluster und alle Replikationsgruppen mithilfe der Regel elasticache-redis-cluster-automatic-backup-check. Der Titel des Steuerelements lautete: Bei (Redis OSS-) Clustern sollten automatische Backups aktiviert sein. ElastiCache Dieses Steuerelement überprüft jetzt zusätzlich zu den Redis OSS-Clustern und allen Replikationsgruppen auch Valkey-Cluster und verwendet dabei die elasticache-automatic-backup-check-enabled-Regel. Der neue Titel und die neue Beschreibung

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		zeigen, dass das Steuerelement beide Clustertypen überprüft .
5. Oktober 2025	Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein	Die Regel für diese Kontrolle wurde aktualisiert, sodass auch ein `PASSED` Ergebnis generiert wird, wenn für eine Amazon OpenSearch Service-Domain keine Softwareupdates verfügbar sind und der Aktualisierungsstatus nicht berechtigt ist. Bisher generiert e diese Kontrolle nur dann ein `PASSED` Ergebnis, wenn für eine OpenSearc h Domain keine Softwareupdates verfügbar waren und der Aktualisierungsstatus abgeschlossen war.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
24. September 2025	[Redshift.9] Redshift-Cluster sollten nicht den Standarddatenbanknamen verwenden [RedshiftServerless.7] Redshift Serverless Namespaces sollten nicht den Standard-Datenbanknamen verwenden	Security Hub CSPM hat diese Kontrollen eingestellt und sie aus allen geltenden Standards entfernt. Security Hub CSPM hat diese Kontrollen aufgrund inhärenter Amazon Redshift Redshift-Einschränkungen eingestellt, die eine effektive Behebung der `FAILED` Kontrollergebnisse verhinderten. Bisher galten die Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) und den Standard NIST SP 800-53 Rev. 5. Die Redshift.9 Kontrolle galt auch für den Service-Managed-Standard.AWS Control Tower

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
9. September 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement nicht mehr `nodejs18.x` als Parameterwert. AWS Lambda unterstützt nicht mehr Node.js 18 Laufzeiten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. August 2025	[SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein	Security Hub CSPM hat den Titel und die Beschreibung dieses Steuerelements geändert. Der neue Titel und die neue Beschreibung geben genauer wieder, dass das Steuerelement die Einstellung für den `EnableNetworkIsolation` Parameter der von Amazon SageMaker AI gehosteten Modelle überprüft. Zuvor lautete der Titel dieses Steuerelements: SageMaker models should block inbound traffic.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
13. August 2025	[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen	Security Hub CSPM hat den Titel und die Beschreibung dieses Steuerelements geändert. Der neue Titel und die neue Beschreibung spiegeln den Umfang und die Art der Prüfung, die die Kontrolle durchführt, genauer wider. Bisher lautete der Titel dieser Kontrolle: EFS mount targets should not be associated with a public subnet.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
24. Juli 2025	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von `1.30` auf geändert. `1.31` Die Standardunterstützung für Kubernetes Version 1.30 in Amazon EKS endete am 23. Juli 2025.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
23. Juli 2025	[EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen	Security Hub CSPM hat den Titel dieses Steuerelements geändert. Der neue Titel spiegelt genauer wider, dass das Steuerelement nur Amazon EC2 Spot Fleet-Anfragen überprüft, die Startparameter angeben. Zuvor lautete der Titel dieses Steuerelements: EC2 Spot Fleet requests should enable encryption for attached EBS volumes.
30. Juni 2025	[IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert	Security Hub CSPM hat dieses Steuerelement aus dem PCI DSS v4.0.1-Standard entfernt. PCI DSS v4.0.1 verlangt nicht ausdrücklich die Verwendung von Symbolen in Passwörtern.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Juni 2025	[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Security Hub CSPM hat dieses Steuerelement aus dem Standard NIST SP 800-171 Revision 2 entfernt. NIST SP 800-171 Revision 2 verlangt nicht ausdrücklich, dass Passwörter innerhalb von 90 Tagen oder weniger ablaufen.
30. Juni 2025	[RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren	Security Hub CSPM hat den Titel dieses Steuerelements geändert. Der neue Titel spiegelt genauer wider, dass das Steuerelement nur Amazon Aurora Aurora-DB-Cluster überprüft. Zuvor lautete der Titel dieses Steuerelements: RDS DB clusters should be configured to copy tags to snapshots.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Juni 2025	[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen	Dieses Steuerelement prüft anhand der für die Notebook-Instance angegebenen Plattform-ID, ob eine Amazon SageMaker AI-Notebook-Instance für die Ausführung auf einer unterstützten Plattform konfiguriert ist. Security Hub CSPM unterstützt `notebook-al2-v1` und nicht mehr `notebook-al2-v2` als Parameterwerte für dieses Steuerelement. Notebook-Instances, die auf diesen Plattformen laufen, haben am 30. Juni 2025 das Ende des Supports erreicht.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Mai 2025	[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein	Security Hub CSPM hat dieses Steuerelement aus dem PCI DSS v4.0.1-Standard entfernt. Dieses Steuerelement prüft, ob die Kontopasswortrichtlinien für IAM-Benutzer die Mindestanforderungen erfüllen, einschließlich einer Mindestkennwortlänge von 7 Zeichen. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Die Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten. Um die Kennwortrichtlinien für Konten anhand der Anforderungen von PCI DSS v4.0.1 zu bewerten, können Sie das Steuerelement verwenden. IAM.7 Für dieses

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Steuerelement müssen Kennwörter mindestens 8 Zeichen lang sein. Es unterstützt auch benutzerdefinierte Werte für die Passwortlänge und andere Parameter. Die IAM.7 Steuerung ist Teil des PCI DSS v4.0.1-Standards in Security Hub CSPM.
8. Mai 2025	[RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden	Security Hub CSPM hat die Freigabe des RDS.46 Steuerelements insgesamt rückgängig gemacht. AWS-Regionen Bisher unterstützte dieses Steuerelement den FSBP-Standard (AWS Foundational Security Best Practices).

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. April 2025	[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden	Dieses Steuerelement prüft, ob der HTTPS-Listener für einen Application Load Balancer oder der TLS-Listener für einen Network Load Balancer so konfiguriert ist, dass Daten während der Übertragung mithilfe einer empfohlenen Sicherheitsrichtlinie verschlüsselt werden. Security Hub CSPM unterstützt jetzt zwei zusätzliche Parameterwerte für dieses Steuerelement: `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` und. `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. März 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement jetzt `ruby3.4` als Parameterwert. AWS Lambda Unterstützung für diese Runtime hinzugefügt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
26. März 2025	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Für den `oldestVersionSupported` Parameter hat Security Hub CSPM den Wert von `1.29` auf geändert. `1.30` Die älteste unterstützte Kubernetes-Version ist jetzt verfügbar. `1.30`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. März 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt `dotnet6` und nicht mehr `python3.8` als Parameterwerte für dieses Steuerelement. AWS Lambda unterstützt diese Laufzeiten nicht mehr.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. März 2025	[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden	Security Hub CSPM hat dieses Steuerelement aus dem Standard „Best Practices für AWS grundlegende Sicherheit“ entfernt und die Überprüfung der Anforderungen von NIST SP 800-53 Rev. 5 automatisiert. Seit der Einstellung von Amazon EC2-Classic Networking können Amazon Relational Database Service (Amazon RDS) -Instances nicht mehr außerhalb einer VPC bereitgestellt werden.
10. Januar 2025	[Glue.2] Bei AWS Glue-Jobs sollte die Protokollierung aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt.
20. Dezember 2024	EC2.61 durch EC2.169	Security Hub CSPM hat die Veröffentlichung der EC2.61 EC2.169 Durchgangskontrollen rückgängig gemacht.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. Dezember 2024	[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden	RDS.23 prüft, ob ein Amazon Relationa l Database Service (Amazon RDS) - Cluster oder eine Instance einen anderen Port als den Standardport der Datenbank-Engine verwendet. Wir haben das Steuerelement aktualisiert, sodass die zugrunde liegende AWS Config Regel `NOT_APPLICABLE` für RDS-Instances, die Teil eines Clusters sind, das Ergebnis von zurückgibt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
2. Dezember 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `nodejs22.x` als Parameter.
26. November 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist jetzt. `1.29`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. November 2024	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressource naufzeichnung verwenden	Config.1 prüft, ob aktiviert AWS Config ist, verwendet die serviceverknüpfte Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM erhöhte den Schweregrad dieser Kontrolle von `MEDIUM` auf `CRITICAL` Security Hub CSPM fügte außerdem neue Statuscodes und Statusgründe für fehlgeschlagene Config.1 Ergebnisse hinzu. Diese Änderungen spiegeln die Bedeutung wider, die Config.1 die CSPM-Kontrollen von Security Hub für den Betrieb haben. Wenn Sie AWS Config oder Resource Recording deaktiviert haben, kann es sein, dass Sie falsche Kontrollergebnisse erhalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Um ein `PASSED` Ergebnis für zu erhalten Config.1, aktivieren Sie die Ressourcenaufzeichnung für Ressourcen, die den aktivierten Security Hub CSPM-Steuerelementen entsprechen, und deaktivieren Sie Kontrollen, die in Ihrer Organisation nicht erforderlich sind. Anweisungen zur Konfiguration AWS Config für Security Hub CSPM finden Sie unter. Aktivierung und Konfiguration AWS Config für Security Hub CSPM Eine Liste der Security Hub CSPM-Steuerelemente und der entsprechenden Ressourcen finden Sie unter. Erforderlich AWS Config Ressourcen für Kontrollbefunde

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. November 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 überprüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `python3.13` als Parameter.
11. Oktober 2024	ElastiCache steuert	Die Titel der Steuerelemente für ElastiCache.3, ElastiCache.4 ElastiCache.5, und wurden geändert ElastiCache.7. In Titeln wird Redis OSS nicht mehr erwähnt, da die Steuerelemente auch ElastiCache für Valkey gelten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. September 2024	[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden	Der geänderte Titel des Steuerelements von Application Load Balancer sollte so konfiguriert werden, dass HTTP-Head er gelöscht werden. Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Head er gelöscht werden.
19. August 2024	Der Titel ändert sich an und die Steuerung DMS.12 ElastiCache	Die Titel der Steuerele mente für DMS.12 und ElastiCac he.1 durch wurden geändert ElastiCac he.7. Wir haben diese Titel geändert, um einer Namensänd erung im Service Amazon ElastiCac he (Redis OSS) Rechnung zu tragen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. August 2024	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressource naufzeichnung verwenden	Config.1 prüft, ob aktiviert AWS Config ist, verwendet die dienstbezogene Rolle und zeichnet Ressourcen für aktivierte Kontrolle n auf. Security Hub CSPM hat einen benutzerd efinierten Steuerpar ameter mit dem Namen hinzugefü gt. `includeCo nfigServi ceLinkedR oleCheck` Wenn Sie diesen Parameter auf setzen`false`, können Sie sich von der Überprüfung abmelden, ob die serviceverknüpfte AWS Config Rolle verwendet wird.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Juli 2024	[IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden	Der Titel des Steuerelements wurde von AWS IoT Core Sicherheitsprofilen sollte markiert werden zu AWS IoT Device Defender Sicherheitsprofile sollten markiert werden geändert.
29. Juli 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr `nodejs16.x` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. Juli 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist `1.28`
25. Juni 2024	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden	Dieses Steuerelement überprüft, ob AWS Config es aktiviert ist, verwendet die dienstbezogene Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM hat den Titel der Kontrolle aktualisiert, um widerzuspiegeln, was die Kontrolle bewertet.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. Juni 2024	[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen	Diese Steuerung prüft, ob ein Amazon Aurora MySQL-DB-Cluster so konfiguriert ist, dass er Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Security Hub CSPM hat das Steuerelement aktualisiert, sodass es keine Ergebnisse für Aurora Serverless v1-DB-Cluster generiert.
11. Juni 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist `1.27`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. Juni 2024	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressource naufzeichnung verwenden	Dieses Steuerelement überprüft, ob aktiviert AWS Config ist und ob die AWS Config Ressourcenaufzeich nung aktiviert ist. Bisher führte das Steuerelement nur dann `PASSED` zu einem Ergebnis, wenn Sie die Aufzeichnung für alle Ressourcen konfiguriert hatten. Security Hub CSPM hat das Steuerele ment aktualisiert, sodass ein `PASSED` Ergebnis angezeigt wird, wenn die Aufzeichnung für Ressourcen aktiviert ist, die für aktiviert e Steuerungen erforderlich sind. Das Steuerelement wurde außerdem aktualisi ert, um zu überprüfe n, ob die AWS Config dienstbezogene Rolle verwendet wird, die Berechtigungen zum Aufzeichnen der erforderlichen

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Ressourcen bereitstellt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Mai 2024	[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	Dieses Steuerelement prüft, ob bei einem versionsbasierten Amazon S3-Bucket für allgemeine Zwecke das Löschen mit Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Zuvor ergab die Kontrolle einen `FAILED` Befund für Buckets, die über eine Lifecycle-Konfiguration verfügen. Das Löschen von MFA mit Versionierung kann jedoch nicht für einen Bucket aktiviert werden, der über eine Lifecycle-Konfiguration verfügt. Security Hub CSPM hat die Steuerung aktualisiert, sodass keine Ergebnisse für Buckets mit einer Lifecycle-Konfiguration vorliegen. Die Beschreibung des Steuerelements wurde aktualisiert, um

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		das aktuelle Verhalten widerzuspiegeln.
2. Mai 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes. `1.26`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. April 2024	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein	Der Titel des Steuerelements wurde von „CloudTrail sollte aktiviert“ auf „Mindestens ein CloudTrail Trail sollte aktiviert sein“ geändert. Dieses Steuerelement zeigt derzeit `PASSED` an AWS-Konto , ob für mindestens ein CloudTrail Trail aktiviert ist. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. April 2024	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	Der Titel der Steuerung wurde von Auto Scaling Scaling-Gruppen, die einem Classic Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden, zu Auto Scaling Scaling-G ruppen, die einem Load Balancer zugeordnet sind, ELB-Zustandsprüfun gen verwenden. Dieses Steuerele ment bewertet derzeit Anwendungs-, Gateway-, Netzwerk- und Classic Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzusp iegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
19. April 2024	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	Das Steuerelement überprüft, ob AWS CloudTrail es aktiviert und mit mindesten s einem Multiregi onspfad konfiguriert ist, der Verwaltun gsereignisse für Lese- und Schreibvo rgänge umfasst. Bisher generierte das Steuerelement fälschlicherweise `PASSED` Ergebnisse, wenn ein Konto mit mindestens einem Multiregions-Trail CloudTrail aktiviert und konfiguriert war, auch wenn kein Trail Lese- und Schreibverwaltungs ereignisse aufzeichn ete. Das Steuerele ment generiert jetzt nur noch `PASSED` Ergebnisse, wenn CloudTrail es aktiviert und mit mindesten s einem multiregi onalen Trail konfiguri ert ist, der Verwaltun gsereignisse für Lese-

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		und Schreibvorgänge erfasst.
10. April 2024	[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Athena-Arbeitsgruppen senden Protokolle an Amazon Simple Storage Service (Amazon S3) -Buckets. Amazon S3 bietet jetzt Standardverschlüsselung mit S3-verwalteten Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets.
10. April 2024	[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit von mehr als 1 haben	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Limits für Metadaten-Antwort-Hops für Amazon Elastic Compute Cloud (Amazon EC2) -Instances hängen von der Arbeitslast ab.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Integration von AWS CloudFormation Stacks mit Amazon SNS SNS-Themen ist keine bewährte Sicherheitsmethode mehr. Die Integration wichtiger CloudFormation Stacks mit SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Stacks erforderlich.
10. April 2024	[CodeBuild.5] In CodeBuild Projektum gebungen sollte der privilegierte Modus nicht aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Aktivierung des privilegierten Modus in einem CodeBuild Projekt stellt kein zusätzliches Risiko für die Kundenumgebung dar.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Der Zweck dieser Kontrolle wird durch eine andere Kontrolle abgedeckt ,. [CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
10. April 2024	[SNS.2] Die Protokollierung des Zustellungsstatus sollte für Benachrichtigungen aktiviert werden, die an ein Thema gesendet werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Das Protokollieren des Zustellungsstatus für SNS-Themen ist keine bewährte Sicherheitsmethode mehr. Das Protokollieren des Zustellungsstatus für wichtige SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Themen erforderlich.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices and Service-Managed Standard entfernt:. AWS Control Tower Der Zweck dieser Kontrolle wird durch zwei weitere Kontrollen abgedeckt: und. [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices and Service-Managed Standard entfernt:. AWS Control Tower Es gibt zwar einige Fälle, in denen Ereignisbenachrichtigungen für S3-Buckets nützlich sind, dies ist jedoch keine allgemein anerkannte bewährte Sicherheitsmethode. Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[SNS.1] SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices and Service-Managed Standard entfernt:. AWS Control Tower Standardmäßig verschlüsselt SNS ruhende Themen mit Festplattenverschlüsselung. Weitere Informationen finden Sie unter Datenverschlüsselung. Die Verwendung AWS KMS zur Verschlüsselung von Themen wird als bewährte Sicherheitsmethode nicht mehr empfohlen. Dieses Steuerelement ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. April 2024	[ELB.6] Bei Anwendung, Gateway und Network Load Balancers sollte der Löschschutz aktiviert sein	Der Steuerelementtitel wurde von Application Load Balancer Balancer-Löschschutz aktiviert in Application, Gateway und Network Load Balancer sollten den Löschschutz aktiviert haben geändert. Dieses Steuerelement bewertet derzeit Application, Gateway und Network Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von Verbindungen zu OpenSearch Domänen sollten mit TLS 1.2 verschlüsselt werden in Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden geändert. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu OpenSearch Domänen TLS 1.2 verwendeten. Das Steuerelement stellt nun `PASSED` fest, ob OpenSearch Domänen mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von Connections zu Elasticsearch-Domains geändert und sollte mit TLS 1.2 verschlüsselt werden. Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu Elasticsearch-Domains TLS 1.2 verwendeten. Das Steuerelement stellt nun `PASSED` fest, ob Elasticsearch-Domains mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	Der Titel sollte von der Einstellung „Öffentlichen Zugriff blockieren“ auf die Einstellung „Öffentlichen Zugriff blockieren“ in S3-Allzweck-Buckets geändert werden. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Lesezugriff auf S3-Buckets verbieten . Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Schreibzugriff auf S3-Buckets verbieten . Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein	Die Änderung des Titels von S3-Buckets sollte Anfragen zur Verwendung von Secure Socket Layer erfordern, zu S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	Der geänderte Titel von S3-Berechtigungen, die anderen AWS-Konten in Bucket-Richtlinien gewährt wurden, sollte auf S3-Allzweck-Bucket-Richtlinien beschränkt werden, sollten den Zugriff auf andere einschränken AWS-Konten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Buckets für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Buckets für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	Der Titel sollte von der Einstellung S3-Zugriff blockieren auf Bucket-Ebene zu S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	Der Titel wurde von der Protokollierung des S3-Bucket-Serverzugriffs aktiviert in die Serverzug riffsprotokollierung sollte für S3-Allzweck-Buckets aktiviert sein geändert. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets mit aktiviert er Versionierung sollten Lebenszyk lusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets mit aktiviert er Versionierung Lifecycle-Konfigur ationen haben sollten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Bei der Änderung des Titels von S3-Buckets sollten Ereignisbenachrichtigungen aktiviert sein, bei S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten	Der geänderte Titel von S3-Zugriffskontrollisten (ACLs) sollte nicht zur Verwaltung des Benutzerzugriffs auf Buckets verwendet werden. ACLs sollten nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets sollten die Lebenszyklusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets Lifecycle-Konfigurationen haben sollten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	Bei der Änderung des Titels von S3-Buckets sollte Versionierung verwendet werden, bei S3-Buckets für allgemeine Zwecke sollte die Versionierung aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein	Der geänderte Titel von S3-Buckets sollte so konfiguriert werden, dass Object Lock verwendet wird. Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	Der Titel wurde von S3-Buckets sollten im Ruhezustand mit AWS KMS keys verschlüsselt werden in S3-Buckets für allgemeine Zwecke geändert. AWS KMS keys Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. März 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `nodejs20.x` und `ruby3.3` als Parameter.
22. Februar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `dotnet8` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Februar 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes. `1.25`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. Januar 2024	[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten	Geänderte Titel- URLs CodeBuild GitHub oder Bitbucket -Quell-Repository- URLs sollten OAuth verwenden, sodass CodeBuild Bitbucket -Quell-Repository- URLs keine vertrauli chen Anmeldein formationen enthalten sollten. Security Hub CSPM hat die Erwähnung von OAuth entfernt, da auch andere Verbindungsmethode n sicher sein können. Security Hub CSPM hat die Erwähnung davon entfernt, GitHub weil es nicht mehr möglich ist, ein persönliches Zugriffstoken oder einen Benutzernamen und ein Passwort in den GitHub Quell- Repository-URLs zu haben.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Januar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt `go1.x` und nicht mehr `java8` als Parameter, da es sich dabei um ausgemusterte Laufzeiten handelt.
29. Dezember 2023	[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	RDS.8 prüft, ob für eine Amazon RDS-DB-Instance, die eine der unterstützten Datenbank-Engines verwendet, der Löschschutz aktiviert ist. Security Hub CSPM unterstützt jetzt `custom-oracle-eeoracle-ee-cdb` , und `oracle-se2-cdb` als Datenbank-Engines.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. Dezember 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 überprüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `java21` und `python3.12` als Parameter. Security Hub CSPM unterstützt nicht mehr `ruby2.7` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. Dezember 2023	Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	CloudFront.1 prüft, ob für eine CloudFront Amazon-Distribution ein Standard-Root-Objekt konfiguriert ist. Security Hub CSPM hat den Schweregrad dieser Kontrolle von CRITICAL auf HIGH herabgesetzt, da das Hinzufügen des Standard-Root-Objekts eine Empfehlung ist, die von der Anwendung und den spezifischen Anforderungen des Benutzers abhängt.
05. Dezember 2023	[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22	Der Titel des Steuerelements wurde von Sicherheitsgruppen geändert und sollte ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 ab Version 0.0.0 auf Port 22 zu Sicherheitsgruppen sollten keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 22.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389	Der Titel des Steuerelements wurde von Version 0.0.0 von „Sicherstellen, dass keine Sicherheitsgruppen den Zugriff zulassen“ geändert. 0/0 ab Version 0.0.0 auf Port 3389 auf Sicherheitsgruppen sollten keinen Zugriff zulassen. 0/0 oder: :/0 auf Port 3389.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen	Der Titel des Steuerelements wurde von Datenbank protokollierung aktiviert zu RDS-DB-Instances sollten Protokolle in Logs veröffentlichen. CloudWatch Security Hub CSPM hat festgestellt, dass dieses Steuerele ment nur prüft, ob Protokolle in Amazon CloudWatch Logs veröffentlicht werden, und nicht, ob RDS-Protokolle aktiviert sind. Die Steuerung stellt `PASSED` fest, ob RDS-DB-Instances so konfiguriert sind, dass sie Protokolle in Logs veröffentlichen. CloudWatch Der Titel des Steuerelements wurde aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein	Diese Steuerung prüft, ob bei Amazon EKS-Clustern die Auditprotokollierung aktiviert ist. Die AWS Config Regel, die Security Hub CSPM zur Auswertung dieser Kontrolle verwendet, wurde von `eks-cluster-logging-enabled` zu geändert. `eks-cluster-log-enabled`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. November 2023	[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	EC2.19 überprüft , ob uneingesc hränkter eingehender Datenverkehr für eine Sicherheitsgruppe über die angegeben en Ports zugänglic h ist, die als risikorei ch eingestuft werden. Security Hub CSPM hat dieses Steuerele ment aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherhei tsgruppenregel bereitgestellt werden. Das Steuerele ment ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0 enthalten. `FAILED` 0/0' oder ': :/0'.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein	Der Titel der Steuerung wurde von CloudWatch Alarmen, für die eine Aktion für den ALARM-Sta tus konfiguriert sein sollte, zu CloudWatc h Alarmen geändert, bei denen bestimmte Aktionen konfiguriert sein sollten.
16. November 2023	[CloudWatch.16] CloudWatch Protokoll gruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	Der geänderte Kontrolltitel aus CloudWatch Protokoll gruppen sollte mindestens ein Jahr lang aufbewahrt werden, während CloudWatch Protokoll gruppen für einen bestimmten Zeitraum aufbewahrt werden sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	Der Titel der Steuerung wurde von VPC-Lambda-Funktionen sollten in mehr als einer Availability Zone funktionieren, in VPC-Lambda-Funktionen geändert, die in mehreren Availability Zones funktionieren sollten.
16. November 2023	[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	Der Titel des Steuerelements wurde von AWS AppSync sollte die Protokollierung auf Anfrage- und Feldebene aktiviert haben in Die Protokollierung auf Feldebene sollte aktiviert sein geändert.AWS AppSync

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	Der Kontrolltitel wurde von Amazon Elastic MapReduce Cluster-Masterknoten sollten keine öffentlichen IP-Adressen haben zu Amazon EMR-Cluster-Primärknoten sollten keine öffentlic hen IP-Adressen haben.
16. November 2023	[Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein	Der Titel der Steuerung wurde von OpenSearch Domänen, die sich in einer VPC befinden sollten, zu OpenSearc hDomänen geändert, die nicht öffentlic h zugänglich sein sollten.
16. November 2023	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein	Der Titel des Steuerelements wurde von Elasticse arch-Domains in einer VPC geändert und Elasticsearch-Domains sollten nicht öffentlich zugänglich sein.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Oktober 2023	[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch	ES.4 prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie Fehlerprotokolle an Amazon CloudWatch Logs senden. Die Kontrolle ergab zuvor einen PASSED Befund für eine Elasticsearch-Domain, deren Logs so konfiguriert sind, dass sie an CloudWatch Logs gesendet werden. Security Hub CSPM hat das Steuerelement aktualisiert, sodass nur ein PASSED Ergebnis für eine Elasticsearch-Domain generiert wird, die so konfiguriert ist, dass sie Fehlerprotokolle an Logs sendet. CloudWatch Das Steuerelement wurde außerdem aktualisiert, um Elasticsearch-Versionen, die Fehlerprotokolle nicht unterstützen,

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		von der Auswertung auszuschließen.
16. Oktober 2023	[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22	EC2.13 prüft, ob Sicherheitsgruppen uneingeschränkten Eingangszugriff auf Port 22 zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0 enthalten. `FAILED` 0/0' oder ': :/0'.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389	EC2.14 prüft, ob Sicherheitsgruppen uneingeschränkten Eingangszugriff auf Port 3389 zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0 enthalten. `FAILED` 0/0' oder ': :/0'.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen	EC2.18 prüft, ob die verwendeten Sicherheitsgruppen uneingeschränkten eingehenden Verkehr zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0.0/0' oder '::/0'. enthalten. `FAILED`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `python3.11` als Parameter.
04. Oktober 2023	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Security Hub CSPM hat den Parameter `ReplicationType` mit dem Wert von hinzugefügt, `CROSS-REGION` um sicherzustellen, dass bei S3-Buckets die regionsübergreifende Replikation aktiviert ist und nicht die Replikation derselben Region.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. September 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes. `1.24`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[CloudFront.2] Bei CloudFront Distributionen sollte die Origin-Zugriffsidentität aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Folgen Sie stattdessen der Anleitung unter [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden. Die Zugriffskontrolle von Origin ist derzeit die bewährte Methode im Bereich Sicherheit. Diese Kontrolle wird innerhalb von 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices (FSBP) und SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) entfernt. Es ist immer noch Teil von Standard: . Service-Managed AWS Control Tower Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2-Instances oder an eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2-Steuerelemente wie EC2.2,, und verwenden EC2.13 EC2.14

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		EC2.18, um Ihre Sicherheitsgruppen zu überwachen EC2.19.
20. September 2023	[EC2.29] EC2-Instances sollten in einer VPC gestartet werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon EC2 hat EC2-Classic Instances zu einer VPC migriert. Dieses Steuerelement wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[S3.4] Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon S3 bietet jetzt Standardverschlüsselung mit S3-verwalteten Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets. Die Verschlüsselungseinstellungen für bestehende Buckets, die mit SS3-S3 oder SS3-KMS serversei tiger Verschlüsselung verschlüsselt sind, sind unverändert. Dieses Steuerelement wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	Der Titel des Steuerelements wurde von Die VPC-Standardsicherheitsgruppe sollte keinen eingehenden und ausgehenden Datenverkehr zulassen zu VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen geändert.
14. September 2023	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	Der Steuertitel wurde von Virtual MFA sollte für den Root-Benutzer aktiviert sein zu MFA sollte für den Root-Benutzer aktiviert sein geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Clusterereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankinstanzereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Datenbankinstanzereignisse konfiguriert werden geändert.
14. September 2023	[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten	Der Titel des Steuerelements wurde von „Eine WAF-Regionalregel sollte mindestens eine Bedingung haben“ in „AWS WAF Klassische regionale Regeln“ geändert, die mindestens eine Bedingung haben sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben	Der Kontrolltitel wurde von einer regionale n WAF-Regelgruppe sollte mindestens eine Regel enthalten zu einer AWS WAF klassischen regionalen Regelgrup pe geändert, die mindestens eine Regel haben sollte.
14. September 2023	[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Kontrolltitel wurde von Eine regionale WAF-Web-ACL sollte mindesten s eine Regel oder Regelgruppe haben in AWS WAF Klassisch e regionale Web-ACLs geändert, die mindestens eine Regel oder Regelgrup pe haben sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regel sollte mindestens eine Bedingung haben“ zu „AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben“ geändert.
14. September 2023	[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regelgruppe sollte mindestens eine Regel haben“ zu „AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben“ geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Steuerelementtitel wurde von Eine globale WAF-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben in AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben geändert.
14. September 2023	[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Kontrolltitel wurde von „Eine WAFv2-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben“ zu „AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben“ geändert.
14. September 2023	[WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein	Der Kontrolltitel wurde von AWS WAF v2-Web-ACL-Protokollierung in AWS WAF Web-ACL-Protokollierung sollte aktiviert sein geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. Juli 2023	[S3.4] Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	S3.4 prüft, ob für einen Amazon S3 S3-Bucket entweder die serverseitige Verschlüsselung aktiviert ist oder ob die S3-Bucket-Richtlinie `PutObject` Anfragen ohne serverseitige Verschlüsselung explizit ablehnt. Security Hub CSPM hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschl üsselung mit KMS-Schlüsseln (). DSSE-KMS Wenn ein S3-Bucket mit, oder verschlüsselt ist, gibt das Steuerelement ein passendes SSE-S3 Ergebnis aus. SSE-KMS DSSE-KMS

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. Juli 2023	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	S3.17 prüft, ob ein Amazon S3 S3-Bucket mit einem verschlüsselt ist AWS KMS key. Security Hub CSPM hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschlüsselung mit KMS-Schlüsseln (). DSSE-KMS Wenn ein S3-Bucket mit oder verschlüsselt ist, gibt das Steuerelement ein passendes Ergebnis aus. SSE-KMS DSSE-KMS
9. Juni 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	EKS.2 prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version läuft. Die älteste unterstützte Version ist jetzt `1.23`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
9. Juni 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `ruby3.2` als Parameter.
5. Juni 2023	[APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	APIGateway.5.checks ob alle Methoden in den REST-API-Stufen von Amazon API Gateway im Ruhezustand verschlüsselt sind. Security Hub CSPM hat das Steuerelement aktualisiert, sodass die Verschlüsselung einer bestimmten Methode nur ausgewertet wird, wenn das Caching für diese Methode aktiviert ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `java17` als Parameter.
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr `nodejs12.x` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
23. April 2023	[ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen	ECS.10 prüft, ob auf den Amazon ECS Fargate-D iensten die neueste Version der Fargate-Plattform ausgeführ t wird. Kunden können Amazon ECS direkt über ECS oder mithilfe von ECS bereitste llen CodeDeploy. Security Hub CSPM hat dieses Steuerele ment aktualisiert, sodass es bei der Bereitstellung von ECS CodeDeploy Fargate-Diensten die Ergebnisse bestanden hat.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. April 2023	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	S3.6 prüft, ob eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) verhindert, dass Prinzipale AWS-Konten anderer Benutzer verweigerte Aktionen für Ressourcen im S3-Bucket ausführen. Security Hub CSPM hat die Steuerung aktualisiert, um Bedingungen in einer Bucket-Richtlinie zu berücksichtigen.
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten den erwarteten Werten entsprechen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt `python3.10` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr `dotnetcore3.1` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. April 2023	[RDS.11] Für RDS-Instances sollten automatische Backups aktiviert sein	RDS.11 prüft, ob für Amazon RDS-Instances automatische Backups aktiviert sind, wobei die Aufbewahrungsfrist für Backups mindestens sieben Tage beträgt. Security Hub CSPM hat diese Kontrolle aktualisiert, um Read Replicas von der Evaluierung auszuschließen, da nicht alle Engines automatische Backups auf Read Replicas unterstützen. Darüber hinaus bietet RDS nicht die Möglichkeit, bei der Erstellung von Read Replicas einen Aufbewahrungszeitraum für Backups anzugeben. Read Replicas werden standardmäßig mit einer Aufbewahrungsdauer für Backups erstellt. `0`

Security Hub CSPM-Steuerungen für AWS-Konten

Diese Security Hub CSPM-Steuerungen werden ausgewertet. AWS-Konten

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.2, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/DE. AE-06.01, CRI-Profil v2. 2/RS. CO-02.01, CRI-Profil v2. 2/RS. CO-02.03

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `security-account-information-provided`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Web Services (AWS) -Konto Sicherheitskontaktinformationen enthält. Die Kontrolle schlägt fehl, wenn keine Sicherheitskontaktinformationen für das Konto bereitgestellt werden.

Alternative Sicherheitskontakte AWS ermöglichen es, eine andere Person bei Problemen mit Ihrem Konto zu kontaktieren, falls Sie nicht verfügbar sind. Benachrichtigungen können von Support oder anderen AWS-Service Teams zu sicherheitsrelevanten Themen im Zusammenhang mit Ihrer AWS-Konto Nutzung stammen.

Abhilfe

Informationen zum Hinzufügen eines alternativen Kontakts als Sicherheitskontakt zu Ihrem AWS-Konto Ansprechpartner finden Sie unter Aktualisieren der alternativen Kontakte für Sie AWS-Konto im Referenzhandbuch zur AWS Kontoverwaltung.

[Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/ID. AM-08.02

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `account-part-of-organizations`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Teil einer Organisation AWS-Konto ist, die über verwaltet wird AWS Organizations. Die Kontrolle schlägt fehl, wenn das Konto nicht Teil einer Organisation ist.

Organizations hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten, während Sie Ihre Workloads skalieren. AWS Sie können mehrere verwenden AWS-Konten , um Workloads zu isolieren, für die bestimmte Sicherheitsanforderungen gelten, oder um Frameworks wie HIPAA oder PCI einzuhalten. Durch die Gründung einer Organisation können Sie mehrere Konten als eine einzige Einheit verwalten und deren Zugriff AWS-Services, Ressourcen und Regionen zentral verwalten.

Abhilfe

Informationen zum Erstellen einer neuen Organisation und AWS-Konten zum automatischen Hinzufügen finden Sie unter Organisation erstellen im AWS Organizations Benutzerhandbuch. Informationen zum Hinzufügen von Konten zu einer bestehenden Organisation finden Sie im AWS Organizations Benutzerhandbuch unter Einladen einer AWS-Konto Person, Ihrer Organisation beizutreten.

Security Hub CSPM-Steuerungen für AWS Amplify

Diese Security Hub CSPM-Steuerungen bewerten den AWS Amplify Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Amplify.1] Amplify-Apps sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Amplify::App`

AWS Config -Regel: amplify-app-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Amplify App über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die App keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die App keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen

mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS Amplify App finden Sie unter Unterstützung für Ressourcen-Tagging im AWS Amplify Hosting-Benutzerhandbuch.

[Amplify.2] Amplify-Zweige sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Amplify::Branch`

AWS Config -Regel: amplify-branch-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	Groß- und Kleinschreibung unterschieden.			

Dieses Steuerelement prüft, ob ein AWS Amplify Zweig über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Zweig keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Zweig keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Amplify Branch finden Sie unter Resource Tagging Support im AWS Amplify Hosting-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon API Gateway

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon API Gateway. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp:`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config -Regel: api-gw-execution-logging-enabled

Zeitplantyp: Änderung ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`loggingLevel`	Protokollierungsstufe	Enum	`ERROR`, `INFO`	`No default value`

Dieses Steuerelement prüft, ob in allen Phasen einer Amazon API Gateway Gateway-REST- oder WebSocket API-Phase die Protokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn `loggingLevel` nicht `ERROR` oder `INFO` für alle Stufen der API. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll,

erzeugt Security Hub CSPM eine erfolgreiche Feststellung, wenn die Protokollierungsebene entweder oder `ERROR` ist. `INFO`

Für API Gateway REST- oder WebSocket API-Stufen sollten die entsprechenden Protokolle aktiviert sein. Die REST- und WebSocket API-Ausführungsprotokollierung von API Gateway bietet detaillierte Aufzeichnungen der Anfragen an die REST- und WebSocket API-Stufen von API Gateway. Die Phasen umfassen Backend-Antworten zur API-Integration, Antworten des Lambda-Autorisierers und die `requestId` For-Integrationsendpunkte. AWS

Abhilfe

Informationen zum Aktivieren der Protokollierung für REST- und WebSocket API-Operationen finden Sie unter CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten im API Gateway Developer Guide.

[APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15, CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: api-gw-ssl-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die REST-API-Stufen von Amazon API Gateway SSL-Zertifikate konfiguriert sind. Backend-Systeme verwenden diese Zertifikate, um zu authentifizieren, dass eingehende Anfragen von API Gateway stammen.

API Gateway REST API-Stufen sollten mit SSL-Zertifikaten konfiguriert werden, damit Backend-Systeme authentifizieren können, dass Anfragen von API Gateway stammen.

Abhilfe

Detaillierte Anweisungen zum Generieren und Konfigurieren von API Gateway REST API-SSL-Zertifikaten finden Sie unter Generieren und Konfigurieren eines SSL-Zertifikats für die Backend-Authentifizierung im API Gateway Developer Guide.

[APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CA-7, CRI Profile v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: api-gw-xray-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS X-Ray Active Tracing für Ihre Amazon API Gateway Gateway-REST-API-Stufen aktiviert ist.

X-Ray Aktives Tracing ermöglicht eine schnellere Reaktion auf Leistungsänderungen in der zugrunde liegenden Infrastruktur. Leistungsänderungen könnten zu einer mangelnden Verfügbarkeit der API führen. X-RayActive Tracing bietet Echtzeit-Metriken zu Benutzeranfragen, die über Ihre API-Gateway-REST-API-Operationen und verbundenen Dienste fließen.

Abhilfe

Detaillierte Anweisungen zur Aktivierung von X-Ray Active Tracing für API Gateway REST API-Operationen finden Sie unter Amazon API Gateway Active Tracing Support for AWS X-Ray im AWS X-Ray Developer Guide.

[APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.03

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: api-gw-associated-with-waf

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein API-Gateway-Schritt eine AWS WAF Web Access Control List (ACL) verwendet. Dieses Steuerelement schlägt fehl, wenn keine AWS WAF Web-ACL an eine REST-API-Gateway-Stufe angehängt ist.

AWS WAF ist eine Firewall für Webanwendungen, die hilft, Webanwendungen und APIs vor Angriffen zu schützen. Damit können Sie eine ACL konfigurieren. Dabei handelt es sich um eine Reihe von Regeln, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre API-Gateway-Stufe mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zur Verwendung der API Gateway-Konsole zum Zuordnen einer AWS WAF regionalen Web-ACL zu einer vorhandenen API-Gateway-API-Stufe finden Sie unter Verwenden AWS WAF zum Schutz Ihrer APIs im API Gateway Developer Guide.

[APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config Regel: `api-gw-cache-encrypted` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob alle Methoden in API Gateway REST API-Stufen, für die der Cache aktiviert ist, verschlüsselt sind. Die Steuerung schlägt fehl, wenn eine Methode in einer API-Gateway-REST-API-Stufe für den Cache konfiguriert ist und der Cache nicht verschlüsselt ist. Security Hub CSPM bewertet die Verschlüsselung einer bestimmten Methode nur, wenn das Caching für diese Methode aktiviert ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff unberechtigter Benutzer auf die Daten einzuschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

API-Gateway-REST-API-Caches sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration von API-Caching für eine Phase finden Sie unter Amazon API Gateway Gateway-Caching aktivieren im API Gateway Developer Guide. Wählen Sie in den Cache-Einstellungen die Option Cache-Daten verschlüsseln.

[APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI Profile v2. 2/PR. IR-01.02

Kategorie: Schützen > Sicheres Zugriffsmanagement

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGatewayV2::Route`

AWS Config -Regel: api-gwv2-authorization-type-configured

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`authorizationType`	Autorisierungstyp der API-Routen	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Kein Standardwert

Diese Kontrolle prüft, ob Amazon API Gateway Gateway-Routen einen Autorisierungstyp haben. Die Steuerung schlägt fehl, wenn die API-Gateway-Route keinen Autorisierungstyp hat. Optional können Sie einen benutzerdefinierten Parameterwert angeben, wenn das Steuerelement nur dann übergeben werden soll, wenn die Route den im `authorizationType` Parameter angegebenen Autorisierungstyp verwendet.

API Gateway unterstützt mehrere Mechanismen zur Steuerung und Verwaltung des Zugriffs auf Ihre API. Durch die Angabe eines Autorisierungstyps können Sie den Zugriff auf Ihre API auf autorisierte Benutzer oder Prozesse beschränken.

Abhilfe

Informationen zum Festlegen eines Autorisierungstyps für HTTP-APIs finden Sie unter Steuern und Verwalten des Zugriffs auf eine HTTP-API in API Gateway im API Gateway Developer Guide. Informationen zum Festlegen eines Autorisierungstyps für WebSocket APIs finden Sie unter Steuern und Verwalten des Zugriffs auf eine WebSocket API in API Gateway im API Gateway Developer Guide.

[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10,, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGatewayV2::Stage`

AWS Config -Regel: api-gwv2-access-logs-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung konfiguriert haben. Diese Kontrolle schlägt fehl, wenn die Einstellungen für das Zugriffsprotokoll nicht definiert sind.

API Gateway Gateway-Zugriffsprotokolle enthalten detaillierte Informationen darüber, wer auf Ihre API zugegriffen hat und wie der Anrufer auf die API zugegriffen hat. Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Aktivieren Sie diese Zugriffsprotokolle, um Verkehrsmuster zu analysieren und Probleme zu beheben.

Weitere bewährte Methoden finden Sie unter Monitoring REST APIs im API Gateway Developer Guide.

Abhilfe

Informationen zum Einrichten der Zugriffsprotokollierung finden Sie unter CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten im API Gateway Developer Guide.

[APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGatewayV2::Integration`

AWS Config -Regel: apigatewayv2-integration-private-https-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei einer API Gateway V2-Integration HTTPS für private Verbindungen aktiviert ist. Die Steuerung schlägt fehl, wenn für eine private Verbindung kein TLS konfiguriert ist.

VPC-Links verbinden API Gateway mit privaten Ressourcen. VPC-Links stellen zwar private Konnektivität her, verschlüsseln Daten jedoch nicht von Natur aus. Durch die Konfiguration von TLS wird die Verwendung von HTTPS für die Ende-zu-Ende-Verschlüsselung vom Client über das API Gateway bis zum Backend sichergestellt. Ohne TLS fließt sensibler API-Verkehr unverschlüsselt über private Verbindungen. Die HTTPS-Verschlüsselung schützt den Datenverkehr über private Verbindungen vor dem Abfangen von Daten, Man-in-the-Middle-Angriffen und der Offenlegung von Anmeldeinformationen.

Abhilfe

Informationen zum Aktivieren der Verschlüsselung während der Übertragung für private Verbindungen in einer API Gateway v2-Integration finden Sie unter Aktualisieren einer privaten Integration im Amazon API Gateway Developer Guide. Konfigurieren Sie die TLS-Konfiguration so, dass die private Integration das HTTPS-Protokoll verwendet.

[APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden

Kategorie: Schützen > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::DomainName`

AWS Config -Regel: apigateway-domain-name-tls-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `allowedSecurityPolicies`: `SecurityPolicy_TLS13_1_3_2025_09, SecurityPolicy_TLS13_1_3_FIPS_2025_09, SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09, SecurityPolicy_TLS13_2025_EDGE, SecurityPolicy_TLS12_PFS_2025_EDGE` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein API-Gateway-Domänenname so konfiguriert ist, dass Daten während der Übertragung mithilfe einer empfohlenen Sicherheitsrichtlinie verschlüsselt werden. Die Steuerung schlägt fehl, wenn der API-Gateway-Domänenname nicht für die Verwendung einer empfohlenen Sicherheitsrichtlinie konfiguriert ist.

Dieses Steuerelement generiert einen `FAILED` Befund für benutzerdefinierte Domainnamen, die an HTTP-APIs angehängt sind. Wenn Sie einen legitimen Anwendungsfall für HTTP-APIs haben, können Sie den Befund unterdrücken.

Eine Sicherheitsrichtlinie ist eine vordefinierte Kombination aus der TLS-Mindestversion und den Verschlüsselungssuites, die von API Gateway angeboten werden. Wenn Ihre Clients einen TLS-Handshake mit Ihrer API oder Ihrem benutzerdefinierten Domain-Namen erfordern, setzt die Sicherheitsrichtlinie die TLS-Version und die Verschlüsselungssuite durch, die von API Gateway akzeptiert werden. Sicherheitsrichtlinien schützen Ihre APIs und benutzerdefinierten Domain-Namen vor Netzwerksicherheitsproblemen wie Manipulationen und Eavesdropping zwischen Client und Server. Die Verwendung einer empfohlenen Sicherheitsrichtlinie trägt dazu bei, dass API-Gateway-Domainnamen moderne, sichere TLS-Konfigurationen verwenden, die Daten bei der Übertragung zwischen Clients und Ihrer API schützen.

Abhilfe

Informationen zur Aktualisierung der TLS-Sicherheitsrichtlinie für einen API Gateway Gateway-Domainnamen finden Sie unter So ändern Sie eine Sicherheitsrichtlinie im Amazon API Gateway Gateway-Entwicklerhandbuch.

Security Hub CSPM-Steuerungen fürAWS AppConfig

Diese Security Hub CSPM-Steuerungen bewerten den AWS AppConfig Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::Application`

AWS Config-Regel: `appconfig-application-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppConfig Anwendung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Anwendung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Anwendung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Anwendung finden Sie TagResourcein der AWS AppConfigAPI-Referenz.

[AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::ConfigurationProfile`

AWS Config-Regel: `appconfig-configuration-profile-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS AppConfig Konfigurationsprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn das Konfigurationsprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Konfigurationsprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS AppConfig Konfigurationsprofil finden Sie TagResourcein der AWS AppConfigAPI-Referenz.

[AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::Environment`

AWS Config-Regel: `appconfig-environment-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppConfig Umgebung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Umgebung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Umgebung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Umgebung finden Sie TagResourcein der AWS AppConfigAPI-Referenz.

[AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::ExtensionAssociation`

AWS Config-Regel: `appconfig-extension-association-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		AWSAnforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine AWS AppConfig Erweiterungsassoziation Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Erweiterungszuordnung keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Erweiterungsverknüpfung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services,

darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Erweiterungsverknüpfung finden Sie TagResourcein der AWS AppConfigAPI-Referenz.

Security Hub CSPM-Steuerungen für Amazon AppFlow

Diese Security Hub CSPM-Kontrollen bewerten den AppFlow Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AppFlow.1] AppFlow Amazon-Flows sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppFlow::Flow`

AWS Config -Regel: `appflow-flow-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß-	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AppFlow Amazon-Flow Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Flow keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Flow mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AppFlow Amazon-Flow finden Sie unter Erstellen von Flows AppFlow in Amazon im AppFlow Amazon-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS App Runner

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS App Runner Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AppRunner.1] App Runner-Dienste sollten markiert sein

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppRunner::Service`

AWS Config -Regel: apprunner-service-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS App Runner Service über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt

fehl, wenn der App Runner-Dienst keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der App Runner-Dienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS App Runner Service finden Sie TagResourcein der AWS App Runner API-Referenz.

[AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppRunner::VpcConnector`

AWS Config -Regel: apprunner-vpc-connector-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS App Runner VPC-Connector Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn der VPC-Connector keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel hat. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der VPC-Connector mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere

Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS App Runner VPC-Connector finden Sie TagResourcein der AWS App Runner API-Referenz.

Security Hub CSPM-Steuerungen für AWS AppSync

Diese Security Hub CSPM-Steuerungen bewerten den AWS AppSync Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

Verwandte Anforderungen: PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: `appsync-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`fieldLoggingLevel`	Ebene der Feldprotokollierung	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	No `default value`

Dieses Steuerelement prüft, ob für eine AWS AppSync API die Protokollierung auf Feldebene aktiviert ist. Das Steuerelement schlägt fehl, wenn die Protokollebene des Field Resolvers auf Keine gesetzt ist. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll, erzeugt Security Hub CSPM einen erfolgreichen Befund, wenn die Protokollebene des Feldauflösers entweder oder ist. `ERROR` `ALL`

Sie können die Protokollierung und Metriken verwenden, um Ihre GraphQL-Abfragen zu identifizieren, Fehler darin zu beheben und sie zu optimieren. Wenn Sie die Protokollierung für AWS AppSync GraphQL aktivieren, erhalten Sie detaillierte Informationen zu API-Anfragen und -Antworten, können Probleme identifizieren und darauf reagieren und gesetzliche Anforderungen erfüllen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für AWS AppSync finden Sie unter Einrichtung und Konfiguration im AWS AppSync Entwicklerhandbuch.

[AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config Regel: `tagged-appsync-graphqlapi` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppSync GraphQL-API Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die GraphQL-API keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die GraphQL-API mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppSync GraphQL-API finden Sie TagResourcein der AWS AppSync API-Referenz.

[AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Hoch

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: `appsync-authorization-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Anwendung einen API-Schlüssel verwendet, um mit einer AWS AppSync GraphQL-API zu interagieren. Die Steuerung schlägt fehl, wenn eine AWS AppSync GraphQL-API mit einem API-Schlüssel authentifiziert wird.

Ein API-Schlüssel ist ein fest codierter Wert in Ihrer Anwendung, der vom AWS AppSync Dienst generiert wird, wenn Sie einen nicht authentifizierten GraphQL-Endpunkt erstellen. Wenn dieser

API-Schlüssel kompromittiert ist, ist Ihr Endpunkt anfällig für unbeabsichtigten Zugriff. Sofern Sie keine öffentlich zugängliche Anwendung oder Website unterstützen, empfehlen wir nicht, einen API-Schlüssel zur Authentifizierung zu verwenden.

Abhilfe

Informationen zum Einrichten einer Autorisierungsoption für Ihre AWS AppSync GraphQL-API finden Sie unter Autorisierung und Authentifizierung im AWS AppSync Entwicklerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Athena

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Athena. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Athena::DataCatalog`

AWS Config Regel: `tagged-athena-datacatalog` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Athena Athena-Datenkatalog Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Datenkatalog keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Datenkatalog mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Athena-Datenkatalog finden Sie unter Tagging Athena-Ressourcen im Amazon Athena Athena-Benutzerhandbuch.

[Athena.3] Athena-Arbeitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Athena::WorkGroup`

AWS Config Regel: `tagged-athena-workgroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine Amazon Athena Athena-Arbeitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Arbeitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Arbeitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Athena-Arbeitsgruppe finden Sie unter Hinzufügen und Löschen von Stichwörtern in einer einzelnen Arbeitsgruppe im Amazon Athena Athena-Benutzerhandbuch.

[Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. IR-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Athena::WorkGroup`

AWS Config -Regel: athena-workgroup-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon Athena Athena-Arbeitsgruppe die Protokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für die Arbeitsgruppe die Protokollierung nicht aktiviert ist.

In Auditprotokollen werden Systemaktivitäten verfolgt und überwacht. Sie bieten eine Aufzeichnung von Ereignissen, anhand derer Sie Sicherheitsverletzungen erkennen, Vorfälle untersuchen und

Vorschriften einhalten können. Auditprotokolle verbessern auch die allgemeine Rechenschaftspflicht und Transparenz Ihres Unternehmens.

Abhilfe

Informationen zur Aktivierung der Protokollierung für eine Athena-Arbeitsgruppe finden Sie unter Aktivieren von CloudWatch Abfragemetriken in Athena im Amazon Athena Athena-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS Backup

Diese Security Hub CSPM-Steuerungen bewerten den AWS Backup Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CP-9 (8) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::Backup::RecoveryPoint`

AWS Config -Regel: `backup-recovery-point-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der Erholungspunkt im Ruhezustand nicht verschlüsselt ist.

Ein AWS Backup Wiederherstellungspunkt bezieht sich auf eine bestimmte Kopie oder einen Snapshot von Daten, der im Rahmen eines Backup-Vorgangs erstellt wird. Er stellt einen bestimmten Zeitpunkt dar, zu dem die Daten gesichert wurden, und dient als Wiederherstellungspunkt für den Fall, dass die Originaldaten verloren gehen, beschädigt werden oder nicht mehr zugänglich sind. Die

Verschlüsselung der Backup-Wiederherstellungspunkte bietet zusätzlichen Schutz vor unbefugtem Zugriff. Die Verschlüsselung ist eine bewährte Methode zum Schutz der Vertraulichkeit, Integrität und Sicherheit von Backup-Daten.

Abhilfe

Informationen zur Verschlüsselung eines AWS Backup Wiederherstellungspunkts finden Sie unter Verschlüsselung für Backups AWS Backup im AWS Backup Entwicklerhandbuch.

[Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::RecoveryPoint`

AWS Config Regel: `tagged-backup-recoverypoint` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Erholungspunkt keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter

angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Kopieren von Tags aus Quellressourcen bei der Erstellung des Backups finden Sie unter Kopieren von Tags auf Backups im AWS Backup Entwicklerhandbuch.

Tags für parent/composite Wiederherstellungspunkte werden bei der Erstellung nicht kopiert. Informationen zum Hinzufügen von Tags zu vorhandenen Wiederherstellungspunkten, einschließlich parent/composite Wiederherstellungspunkten, finden Sie unter Hinzufügen oder Entfernen von Tags auf vorhandenen Wiederherstellungspunkten im AWS Backup Entwicklerhandbuch.

[Backup.3] AWS Backup Tresore sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::BackupVault`

AWS Config Regel: `tagged-backup-backupvault` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Tresor über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Recovery Point keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter angegebenen Schlüssel verfügt`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem hinzu AWS Backup Tresor

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie Neues Tag hinzufügen für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::ReportPlan`

AWS Config Regel: `tagged-backup-reportplan` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Berichtsplan Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Berichtsplan keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Berichtsplan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem hinzu AWS Backup Plan melden

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.5] AWS Backup Backup-Pläne sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::BackupPlan`

AWS Config Regel: `tagged-backup-backupplan` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Backup-Plan Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Backup-Plan keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Backup-Plan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem hinzu AWS Backup Backup-Plan

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

Security Hub CSPM-Steuerungen für AWS Batch

Diese Security Hub CSPM-Steuerungen bewerten den AWS Batch Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Batch.1] Batch-Job-Warteschlangen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::JobQueue`

AWS Config -Regel: batch-job-queue-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Auftragswarteschlange Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Auftragswarteschlange keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Auftragswarteschlange mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Batch-Job-Warteschlange finden Sie unter Taggen Ihrer Ressourcen im AWS Batch Benutzerhandbuch.

[Batch.2] Richtlinien zur Batch-Planung sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::SchedulingPolicy`

AWS Config -Regel: batch-scheduling-policy-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Planungsrichtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Planungsrichtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Scheduling-Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Batch-Planungsrichtlinie finden Sie unter Taggen Ihrer Ressourcen im AWS Batch Benutzerhandbuch.

[Batch.3] Batch-Computing-Umgebungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::ComputeEnvironment`

AWS Config -Regel: batch-compute-environment-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Rechenumgebung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Rechenumgebung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Rechenumgebung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Batch-Computing-Umgebung finden Sie unter Taggen Ihrer Ressourcen im AWS Batch Benutzerhandbuch.

[Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::ComputeEnvironment`

AWS Config -Regel: batch-managed-compute-env-compute-resources-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob die Eigenschaft Compute Resources in einer verwalteten AWS Batch Rechenumgebung über die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die Eigenschaft „Compute Resources“ keine Tag-Schlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn eine Compute-Resources-Eigenschaft keine Tag-Schlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben. Dieses Steuerelement bewertet weder unverwaltete Computerumgebungen noch verwaltete Umgebungen, die Ressourcen verbrauchen AWS Fargate .

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu Rechenressourcen in einer verwalteten AWS Batch Rechenumgebung finden Sie unter Taggen Ihrer Ressourcen im AWS Batch Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Bedrock

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Bedrock. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Bedrock.1] Amazon Bedrock-Datenquellen sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Ressourcentyp: `AWS::Bedrock::DataSource`

AWS Config -Regel: bedrock-data-source-encryption-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon Bedrock-Datenquelle im Ruhezustand mit einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt ist. Die Kontrolle schlägt fehl, wenn die Datenquelle nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Das Steuerelement bewertet keine Datenquellen, die zu einer verwalteten Wissensdatenbank gehören.

Standardmäßig verschlüsselt Amazon Bedrock Datenquelleninhalte mit AWS verwalteten Schlüsseln. Durch die Verwendung eines vom Kunden verwalteten KMS-Schlüssels haben Sie die volle Kontrolle über den Lebenszyklus des Verschlüsselungsschlüssels, einschließlich Rotation, Zugriffsrichtlinien und Überprüfung. AWS CloudTrail Auf diese Weise können Compliance-Anforderungen erfüllt

werden, die eine vom Kunden kontrollierte Verschlüsselung für sensible Daten vorschreiben, die in Wissensdatenbanken aufgenommen werden.

Abhilfe

Informationen zum Verschlüsseln Ihrer Amazon Bedrock-Datenquelle mit einem vom Kunden verwalteten KMS-Schlüssel finden Sie unter Ändern einer Datenquelle für Ihre Amazon Bedrock-Wissensdatenbank im Amazon Bedrock-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Bedrock AgentCore

Diese AWS Security Hub CSPM Kontrollen bewerten den AgentCore Service und die Ressourcen von Amazon Bedrock. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Hoch

Art der Ressource: `AWS::BedrockAgentCore::Runtime`

AWS Config -Regel: bedrockagentcore-runtime-private-network-required

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon AgentCore Bedrock-Laufzeit mit dem VPC-Netzwerkmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Netzwerkmodus der Laufzeit auf PUBLIC gesetzt ist.

Das Steuerelement liefert keine Ergebnisse für Laufzeiten, die von einem Kapazitätsanbieter unterstützt werden. Diese Laufzeiten definieren ihre Netzwerkkonfiguration auf dem Kapazitätsanbieter und nicht auf der Laufzeit, sodass sie nicht in den Anwendungsbereich dieser Kontrolle fallen.

Durch die Verwendung des öffentlichen Netzwerkmodus für Amazon AgentCore Bedrock-Laufzeiten wird die Laufzeit direkt dem Internet ausgesetzt, wodurch die Angriffsfläche und das Risiko eines unbefugten Zugriffs erhöht werden. Durch die Konfiguration von Laufzeiten im VPC-Netzwerkmodus

wird sichergestellt, dass der Laufzeitdatenverkehr auf Ihr privates Netzwerk beschränkt wird, sodass Sie Sicherheitskontrollen auf Netzwerkebene wie Sicherheitsgruppen, Netzwerk-ACLs und VPC-Flussprotokolle anwenden können.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie die nicht konforme AgentCore Bedrock-Laufzeit und konfigurieren Sie sie mit dem VPC-Netzwerkmodus. Anweisungen finden Sie unter Amazon Bedrock AgentCore Runtime und Tools für VPC konfigurieren im Amazon Bedrock AgentCore Developer Guide.

[BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::BedrockAgentCore::Gateway`

AWS Config -Regel: bedrockagentcore-gateway-authorizer-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Bedrock AgentCore Gateway eine Autorisierung für eingehende Anfragen benötigt. Die Kontrolle schlägt fehl, wenn für das Bedrock AgentCore Gateway keine eingehende Autorisierung eingerichtet ist.

Durch die Konfiguration der Authentifizierung auf Amazon Bedrock AgentCore Gateways wird sichergestellt, dass nur autorisierte Kunden Anfragen an Ihre KI-Agenten senden können. Ohne einen Autorisierer kann jede Entität mit Netzwerkzugriff auf den Gateway-Endpunkt Ihre Agenten aufrufen, was möglicherweise zu unbefugtem Datenzugriff, Ressourcenmissbrauch oder unerwarteten Kosten führen kann. Bei der eingehenden Autorisierung werden Benutzer validiert, die versuchen, über Ihr Gateway auf Ziele zuzugreifen. AgentCore

Abhilfe

Informationen zum Einrichten der eingehenden Autorisierung für ein Amazon Bedrock AgentCore Gateway finden Sie unter Einrichten der eingehenden Autorisierung für Ihr Gateway im Amazon AgentCore Bedrock Developer Guide.

[BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::BedrockAgentCore::Memory`

AWS Config -Regel: bedrock-agentcore-memory-encryption-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Bedrock AgentCore Memory im Ruhezustand mit einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt ist. Die Kontrolle schlägt fehl, wenn der Bedrock AgentCore Memory nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist.

Die Verwendung eines vom Kunden verwalteten KMS-Schlüssels für die Verschlüsselung des Amazon AgentCore Bedrock-Speichers bietet mehr Sicherheit als der vom Service verwaltete Standardschlüssel. Mit vom Kunden verwalteten KMS-Schlüsseln haben Sie die volle Kontrolle über den Lebenszyklus und die Zugriffsrichtlinien des Verschlüsselungsschlüssels. Darüber hinaus kann die gesamte Verwendung von Verschlüsselungsschlüsseln protokolliert und aus AWS CloudTrail Gründen der Überprüfbarkeit überwacht werden.

Abhilfe

Informationen zur Verschlüsselung Ihres Amazon Bedrock AgentCore Memory mit einem vom Kunden verwalteten KMS-Schlüssel finden Sie unter Verschlüsseln Ihres Amazon Bedrock AgentCore Memory im Amazon Bedrock Developer Guide. AgentCore

[BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::BedrockAgentCore::Gateway`

AWS Config -Regel: bedrockagentcore-gateway-encryption-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Bedrock AgentCore Gateway im Ruhezustand mit einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt ist. Die Kontrolle schlägt fehl, wenn das Bedrock AgentCore Gateway nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Die Steuerung bewertet nicht, ob der konfigurierte, vom Kunden verwaltete KMS-Schlüssel deaktiviert oder gelöscht ist.

Standardmäßig AgentCore verschlüsselt Amazon Bedrock Gateway-Daten mit AWS verwalteten Schlüsseln. Durch die Verwendung eines vom Kunden verwalteten KMS-Schlüssels haben Sie die volle Kontrolle über den Lebenszyklus des Verschlüsselungsschlüssels, einschließlich Rotation, Zugriffsrichtlinien und Überprüfung. AWS CloudTrail Dies trägt dazu bei, die Compliance-Anforderungen zu erfüllen, die eine vom Kunden kontrollierte Verschlüsselung für sensible KI-Workloads vorschreiben.

Abhilfe

Informationen zur Verschlüsselung Ihres Bedrock AgentCore Gateways mit einem vom Kunden verwalteten KMS-Schlüssel finden Sie unter Verschlüsseln Sie Ihr AgentCore Gateway mit einem vom Kunden verwalteten KMS-Schlüssel im Amazon Bedrock Developer Guide. AgentCore

[BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::BedrockAgentCore::BrowserCustom`

AWS Config -Regel: bedrockagentcore-browsercustom-network-mode-not-public

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AgentCore benutzerdefinierter Amazon Bedrock-Browser mit dem öffentlichen Netzwerkmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Netzwerkmodus auf öffentlich eingestellt ist.

Durch die Verwendung des Netzwerkmodus PUBLIC für AgentCore benutzerdefinierte Browser von Amazon Bedrock werden Browsersitzungen direkt mit dem Internet verbunden, wodurch die Angriffsfläche und das Risiko eines unbefugten Zugriffs erhöht werden. Durch die Konfiguration von Browsern im VPC-Netzwerkmodus wird sichergestellt, dass der Browserverkehr auf Ihr privates Netzwerk beschränkt wird, sodass Sie Sicherheitskontrollen auf Netzwerkebene wie Sicherheitsgruppen, Netzwerk-ACLs und VPC-Flussprotokolle anwenden können.

Abhilfe

Um dieses Problem zu beheben, löschen Sie den nicht kompatiblen AgentCore benutzerdefinierten Bedrock-Browser und erstellen Sie ihn im VPC-Netzwerkmodus neu. Anweisungen finden Sie unter Amazon Bedrock AgentCore Runtime und Tools für VPC konfigurieren im Amazon Bedrock AgentCore Developer Guide.

[BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: `AWS::BedrockAgentCore::BrowserCustom`

AWS Config -Regel: bedrockagentcore-browsercustom-recording-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem AgentCore benutzerdefinierten Amazon Bedrock-Browser die Sitzungsaufzeichnung aktiviert ist und ein S3-Ziel konfiguriert ist. Die Steuerung schlägt fehl, wenn in einem benutzerdefinierten Browser die Aufzeichnung nicht aktiviert ist oder kein S3-Standort für das Speichern von Aufzeichnungen konfiguriert ist.

Die Sitzungsaufzeichnung für AgentCore benutzerdefinierte Bedrock-Browser gewährleistet die vollständige Überprüfbarkeit von Browserinteraktionen und ermöglicht die Erkennung von unbefugtem Zugriff, Datenexfiltration oder böswilligen Aktivitäten während automatisierter Browsersitzungen.

Abhilfe

Anweisungen zur Aktivierung der Browser-Sitzungsaufzeichnung finden Sie unter Sitzungsaufzeichnung und -wiedergabe im Amazon Bedrock AgentCore Developer Guide.

[BedrockAgentCore.7] Bedrock-Interpreter für AgentCore benutzerdefinierten Code sollten eine private Netzwerkkonfiguration verwenden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::BedrockAgentCore::CodeInterpreterCustom`

AWS Config -Regel: bedrockagentcore-codeinterpreter-networkmode-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Bedrock AgentCore Custom Code Interpreter mit einem privaten Netzwerkmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Netzwerkmodus auf `PUBLIC` oder eingestellt ist. `SANDBOX`

Durch die Konfiguration AgentCore benutzerdefinierter Codeinterpreter von Bedrock mit einem privaten Netzwerkmodus wird sichergestellt, dass die Codeausführungsumgebungen innerhalb Ihrer VPC isoliert sind. Im öffentlichen Netzwerkmodus oder im Sandbox-Netzwerkmodus ist der Codeinterpreter dem Internet zugänglich, wodurch das Risiko eines unbefugten Zugriffs und einer Datenexfiltration erhöht wird. Die Verwendung des privaten Netzwerkmodus schränkt den Netzwerkzugriff ein und trägt zum Schutz sensibler Daten bei, die bei der Codeinterpretation verarbeitet werden.

Abhilfe

Um dieses Problem zu beheben, löschen Sie den nicht konformen Bedrock AgentCore Custom Code Interpreter und erstellen Sie ihn im VPC-Netzwerkmodus neu. Anweisungen finden Sie unter

Konfiguration des VPC-Zugriffs für Runtime und Tools im Amazon Bedrock AgentCore Developer Guide.

Security Hub CSPM-Steuerungen für AWS Certificate Manager

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Certificate Manager (ACM) -Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

Verwandte Anforderungen: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ACM::Certificate`

AWS Config -Regel: acm-certificate-expiration-check

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`daysToExpiration`	Anzahl der Tage, innerhalb derer das ACM-Zertifikat erneuert werden muss	Ganzzahl	`14` auf `365`	`30`

Diese Kontrolle prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat innerhalb des angegebenen Zeitraums erneuert wird. Es überprüft sowohl importierte Zertifikate als auch von ACM bereitgestellte

Zertifikate. Die Kontrolle schlägt fehl, wenn das Zertifikat nicht innerhalb des angegebenen Zeitraums erneuert wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Verlängerungszeitraum angeben, verwendet Security Hub CSPM einen Standardwert von 30 Tagen.

ACM kann Zertifikate, die DNS-Validierung verwenden, automatisch verlängern. Bei Zertifikaten, die E-Mail-Validierung verwenden, müssen Sie auf eine E-Mail zur Domainvalidierung antworten. ACM erneuert Zertifikate, die Sie importieren, nicht automatisch. Sie müssen importierte Zertifikate manuell erneuern.

Abhilfe

ACM bietet eine verwaltete Verlängerung für Ihre von Amazon ausgestellten SSL/TLS Zertifikate. Das bedeutet, dass ACM Ihre Zertifikate entweder automatisch erneuert (wenn Sie die DNS-Validierung verwenden) oder Ihnen E-Mail-Benachrichtigungen sendet, wenn der Ablauf des Zertifikats näher rückt. Diese Dienste werden sowohl für öffentliche als auch für private ACM-Zertifikate bereitgestellt.

Für Domains, die per E-Mail validiert wurden

Wenn ein Zertifikat 45 Tage vor Ablauf abläuft, sendet ACM für jeden Domainnamen eine E-Mail an den Domaininhaber. Um die Domains zu validieren und die Verlängerung abzuschließen, müssen Sie auf die E-Mail-Benachrichtigungen antworten.

Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter Verlängerung für per E-Mail validierte Domains.

Für Domains, die durch DNS validiert wurden

ACM erneuert automatisch Zertifikate, die DNS-Validierung verwenden. 60 Tage vor Ablauf überprüft ACM, ob das Zertifikat erneuert werden kann.

Wenn ein Domainname nicht validiert werden kann, sendet ACM eine Benachrichtigung, dass eine manuelle Validierung erforderlich ist. Diese Benachrichtigungen werden 45 Tage, 30 Tage, 7 Tage und 1 Tag vor Ablauf gesendet.

Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter Verlängerung für durch DNS validierte Domains.

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

Verwandte Anforderungen: PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Identifizieren > Inventar > Inventardienste

Schweregrad: Hoch

Art der Ressource: `AWS::ACM::Certificate`

AWS Config -Regel: acm-certificate-rsa-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RSA-Zertifikate, die mit verwaltet werden, eine Schlüssellänge von mindestens 2.048 Bit AWS Certificate Manager verwenden. Die Steuerung schlägt fehl, wenn die Schlüssellänge kleiner als 2.048 Bit ist.

Die Stärke der Verschlüsselung korreliert direkt mit der Schlüsselgröße. Wir empfehlen Schlüssellängen von mindestens 2.048 Bit, um Ihre AWS Ressourcen zu schützen, da Rechenleistung immer günstiger wird und Server immer fortschrittlicher werden.

Abhilfe

Die Mindestschlüssellänge für von ACM ausgestellte RSA-Zertifikate beträgt bereits 2.048 Bit. Anweisungen zur Ausstellung neuer RSA-Zertifikate mit ACM finden Sie unter Ausstellen und Verwalten von Zertifikaten im Benutzerhandbuch.AWS Certificate Manager

Mit ACM können Sie zwar Zertifikate mit kürzeren Schlüssellängen importieren, Sie müssen jedoch Schlüssel mit mindestens 2.048 Bit verwenden, um diese Kontrolle zu bestehen. Sie können die Schlüssellänge nach dem Import eines Zertifikats nicht ändern. Stattdessen müssen Sie Zertifikate mit einer Schlüssellänge von weniger als 2.048 Bit löschen. Weitere Informationen zum Importieren von Zertifikaten in ACM finden Sie unter Voraussetzungen für den Import von Zertifikaten im AWS Certificate Manager Benutzerhandbuch.

[ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ACM::Certificate`

AWS Config Regel: `tagged-acm-certificate` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Kontrolle schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ACM-Zertifikat finden Sie unter Kennzeichnen von AWS Certificate Manager Zertifikaten im Benutzerhandbuch.AWS Certificate Manager

Security Hub CSPM-Steuerungen fürCloudFormation

Diese Security Hub CSPM-Steuerungen bewerten den AWS CloudFormation Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden

> **Important**
>
> Security Hub CSPM hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub CSPM-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFormation::Stack`

AWS Config-Regel: `cloudformation-stack-notification-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon Simple Notification Service-Benachrichtigung in einen CloudFormation Stack integriert ist. Die Kontrolle schlägt für einen CloudFormation Stack fehl, wenn ihm keine SNS-Benachrichtigung zugeordnet ist.

Wenn Sie eine SNS-Benachrichtigung mit Ihrem CloudFormation Stack konfigurieren, können Sie die Beteiligten sofort über alle Ereignisse oder Änderungen informieren, die im Stack auftreten.

Abhilfe

Informationen zur Integration eines CloudFormation Stacks und eines SNS-Themas finden Sie unter Stacks direkt aktualisieren im AWS CloudFormation Benutzerhandbuch.

[CloudFormation.2] CloudFormation Stacks sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFormation::Stack`

AWS ConfigRegel: `tagged-cloudformation-stack` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CloudFormation Stack Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Stack keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Stack mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudFormation Stack finden Sie CreateStackin der AWS CloudFormationAPI-Referenz.

Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFormation::Stack`

AWS Config-Regel: cloudformation-termination-protection-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen AWS CloudFormation Stack der Terminierungsschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Terminierungsschutz für einen CloudFormation Stack nicht aktiviert ist.

CloudFormation hilft dabei, verwandte Ressourcen als eine einzige Einheit zu verwalten, die als Stack bezeichnet wird. Sie können das versehentliche Löschen eines Stacks verhindern, indem Sie den Beendigungsschutz des Stacks aktivieren. Wenn ein Benutzer versucht, einen Stack mit aktiviertem Beendigungsschutz zu löschen, schlägt das Löschen fehl und der Stack – einschließlich seines Status – bleibt unverändert. Sie können den Beendigungsschutz für einen Stapel mit einem beliebigen Status außer `DELETE_IN_PROGRESS` oder `DELETE_COMPLETE`einstellen.

> **Note**
>
> Wenn Sie den Beendigungsschutz für einen Stack aktivieren oder deaktivieren, wird diese Entscheidung auch an alle verschachtelten Stacks weitergegeben, die zu diesem Stack gehören. Sie können den Beendigungsschutz nicht direkt für einen verschachtelten Stack aktivieren oder deaktivieren. Sie können einen verschachtelten Stack, der zu einem Stack gehört, für den der Terminierungsschutz aktiviert ist, nicht direkt löschen. Wenn neben dem Stack-Namen NESTED angezeigt wird, handelt es sich um einen verschachtelten Stack. Sie können nur den Beendigungsschutz des Root-Stacks ändern, zu dem der verschachtelte Stack gehört.

Abhilfe

Informationen zum Aktivieren des Kündigungsschutzes für einen CloudFormation Stack finden Sie unter CloudFormation Stacks vor dem Löschen schützen im AWS CloudFormationBenutzerhandbuch.

[CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben

Kategorie: Erkennen > Sicheres Zugriffsmanagement

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFormation::Stack`

AWS Config-Regel: cloudformation-stack-service-role-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob einem AWS CloudFormation Stack eine Servicerolle zugeordnet ist. Das Steuerelement schlägt für einen CloudFormation Stack fehl, wenn ihm keine Servicerolle zugeordnet ist.

Service-managed StackSets Verwenden Sie Ausführungsrollen über die vertrauenswürdige Zugriffsintegration von AWS Organizations. Das Steuerelement generiert außerdem den Befund FAILED für einen AWS CloudFormation Stack, der von service-managed erstellt wurde, StackSets weil ihm keine Servicerolle zugeordnet ist. Aufgrund der Art der vom Service verwalteten StackSets Authentifizierung kann das `roleARN` Feld für diese Stacks nicht ausgefüllt werden.

Die Verwendung von Servicerollen mit CloudFormation Stacks hilft bei der Implementierung des Zugriffs mit den geringsten Rechten, indem die Berechtigungen zwischen dem Benutzer, der die creates/updates Stapel erstellt, und den Berechtigungen, die für zwei Ressourcen benötigt werden, getrennt werden. CloudFormation create/update Dies reduziert das Risiko einer Eskalation von Rechten und trägt dazu bei, die Sicherheitsgrenzen zwischen verschiedenen betrieblichen Rollen aufrechtzuerhalten.

> **Note**
>
> Es ist nicht möglich, eine Service-Rolle zu entfernen, die einem Stack zugewiesen ist, nachdem der Stack erstellt wurde. Andere Benutzer, die die Berechtigung haben, Operationen auf diesem Stapel durchzuführen, können diese Rolle verwenden, unabhängig davon, ob diese Benutzer die Berechtigung `iam:PassRole` haben oder nicht. Wenn die Rolle Berechtigungen umfasst, die der Benutzer nicht haben sollte, können Sie die Berechtigungen eines Benutzers versehentlich weiterleiten. Stellen Sie sicher, dass die Rolle die geringsten Rechte zugesteht.

Abhilfe

Informationen zum Zuordnen einer Servicerolle zu einem CloudFormation Stack finden Sie unter CloudFormation Servicerolle im AWS CloudFormationBenutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon CloudFront

Diese AWS Security Hub CSPM Kontrollen bewerten den CloudFront Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0. 1/22.2.6, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-default-root-object-configured

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution mit S3-Ursprüngen so konfiguriert ist, dass sie ein bestimmtes Objekt zurückgibt, das das Standard-Root-Objekt ist. Die Steuerung schlägt fehl, wenn die CloudFront Distribution S3-Ursprünge verwendet und kein Standard-Root-Objekt konfiguriert ist. Dieses Steuerelement gilt nicht für CloudFront Distributionen, die benutzerdefinierte Ursprünge verwenden.

Ein Benutzer kann manchmal die Stamm-URL der Distribution anstelle eines Objekts in der Distribution anfordern. In diesem Fall können Sie durch die Festlegung eines Standardstammobjekt verhindern, dass die Inhalte Ihrer Web-Verteilung preisgegeben werden.

Abhilfe

Informationen zur Konfiguration eines Standard-Root-Objekts für eine CloudFront Distribution finden Sie unter How to specify a default root object im Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-viewer-policy-https

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei einer CloudFront Amazon-Distribution Zuschauer HTTPS direkt verwenden müssen oder ob sie eine Umleitung verwendet. Die Steuerung schlägt fehl, wenn sie auf `allow-all` für `defaultCacheBehavior` oder für `cacheBehaviors` gesetzt `ViewerProtocolPolicy` ist.

HTTPS (TLS) kann verwendet werden, um potenzielle Angreifer daran zu hindern, Person-in-the-Middle- oder ähnliche Angriffe zu nutzen, um den Netzwerkverkehr abzuhören oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Verschlüsseln einer CloudFront Verteilung während der Übertragung finden Sie unter HTTPS für die Kommunikation zwischen Zuschauern erforderlich und CloudFront im Amazon CloudFront Developer Guide.

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-origin-failover-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution mit einer Ursprungsgruppe konfiguriert ist, die zwei oder mehr Ursprünge hat.

CloudFront Origin-Failover kann die Verfügbarkeit erhöhen. Origin-Failover leitet den Datenverkehr automatisch an einen sekundären Ursprung weiter, wenn der primäre Ursprung nicht verfügbar ist oder wenn bestimmte HTTP-Antwortstatuscodes zurückgegeben werden.

Abhilfe

Informationen zur Konfiguration des Origin-Failovers für eine CloudFront Distribution finden Sie unter Creating an Origin Group im Amazon CloudFront Developer Guide.

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, (3) NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (9), (8) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-accesslogs-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für CloudFront Distributionen aktiviert ist. Die Steuerung schlägt fehl, wenn die Zugriffsprotokollierung für eine Verteilung nicht aktiviert ist. Dieses Steuerelement bewertet nur, ob die Standardprotokollierung (Legacy) für eine Verteilung aktiviert ist.

CloudFront Zugriffsprotokolle enthalten detaillierte Informationen zu jeder Benutzeranfrage, die bei uns eingeht CloudFront. Jedes Protokoll enthält Informationen wie Datum und Uhrzeit des Eingangs der Anfrage, die IP-Adresse des Betrachters, der die Anfrage gestellt hat, die Quelle der Anfrage und die Portnummer der Anfrage vom Betrachter. Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Weitere Informationen zur Analyse von Zugriffsprotokollen finden Sie unter CloudFront Amazon-Protokolle abfragen im Amazon Athena-Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der Standardprotokollierung (Legacy) für eine CloudFront Distribution finden Sie unter Standardprotokollierung konfigurieren (Legacy) im Amazon CloudFront Developer Guide.

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0. 1/64.4.2, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/GV. OC-04.03, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-associated-with-waf

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen entweder AWS WAF Classic- oder AWS WAF Web-ACLs zugeordnet sind. Das Steuerelement schlägt fehl, wenn die Verteilung keiner Web-ACL zugeordnet ist.

AWS WAF ist eine Firewall für Webanwendungen, die dazu beiträgt, Webanwendungen und APIs vor Angriffen zu schützen. Sie ermöglicht es ihnen, eine Gruppe von Regeln (eine sogenannte Web-Zugriffskontrollliste oder Web-ACL) zum Zulassen, Blockieren oder Zählen von Webanforderungen basierend auf von Ihnen definierten anpassbaren Web-Sicherheitsregeln und Bedingungen zu konfigurieren. Stellen Sie sicher, dass Ihre CloudFront Distribution mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Zuordnen einer AWS WAF Web-ACL zu einer CloudFront Distribution finden Sie unter Verwendung AWS WAF zur Zugriffskontrolle auf Ihre Inhalte im Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15, CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-custom-ssl-certificate

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen die SSL/TLS Standardzertifikate verwenden CloudFront . Diese Kontrolle ist erfolgreich, wenn die CloudFront Verteilung ein benutzerdefiniertes SSL/TLS Zertifikat verwendet. Diese Kontrolle schlägt fehl, wenn die CloudFront Verteilung das SSL/TLS Standardzertifikat verwendet.

Benutzerdefiniert SSL/TLS ermöglichen es Ihren Benutzern, mithilfe alternativer Domainnamen auf Inhalte zuzugreifen. Sie können benutzerdefinierte Zertifikate in AWS Certificate Manager (empfohlen) oder in IAM speichern.

Abhilfe

Informationen zum Hinzufügen eines alternativen Domainnamens für eine CloudFront Distribution mit einem benutzerdefinierten SSL/TLS Zertifikat finden Sie unter Hinzufügen eines alternativen Domainnamens im Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-sni-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen ein benutzerdefiniertes SSL/TLS Zertifikat verwenden und so konfiguriert sind, dass SNI zur Bearbeitung von HTTPS-Anfragen verwendet wird. Diese Kontrolle schlägt fehl, wenn ein benutzerdefiniertes SSL/TLS Zertifikat zugeordnet ist, die SSL/TLS Unterstützungsmethode jedoch eine dedizierte IP-Adresse ist. Die Steuerung schlägt auch fehl, wenn die Verteilung ein CloudFront SSL/TLS Standardzertifikat verwendet.

Die Servernamensanzeige (SNI) ist eine Erweiterung des TLS-Protokolls, die in Browsern und Clients unterstützt wird, die nach 2010 veröffentlicht wurden. Wenn Sie so konfigurieren CloudFront ,

dass HTTPS-Anfragen mithilfe von SNI bedient werden, CloudFront ordnet Sie Ihrem alternativen Domainnamen eine IP-Adresse für jeden Edge-Standort zu. Sobald ein Viewer Inhalte von Ihnen durch Senden einer HTTPS-Anforderung abruft, leitet DNS die Anforderung an die IP-Adresse des korrekten Edge-Standorts weiter. Die IP-Adresse Ihres Domainnamens wird während der SSL/TLS Handshake-Verhandlung festgelegt. Die IP-Adresse ist nicht für Ihre Distribution reserviert.

Abhilfe

Informationen zur Konfiguration einer CloudFront Distribution für die Verwendung von SNI zur Bearbeitung von HTTPS-Anfragen finden Sie unter Verwenden von SNI zur Bearbeitung von HTTPS-Anfragen (funktioniert für die meisten Kunden) im CloudFront Entwicklerhandbuch. Informationen zu benutzerdefinierten SSL-Zertifikaten finden Sie unter Anforderungen für die Verwendung von SSL/TLS Zertifikaten mit. CloudFront

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-traffic-to-origin-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Diese Kontrolle schlägt bei einer CloudFront Distribution fehl, deren Ursprungsprotokollrichtlinie „Nur HTTP“ zulässt. Diese Kontrolle schlägt auch fehl, wenn die Ursprungsprotokollrichtlinie der Distribution „Match-Viewer“ lautet, während die Viewer-Protokollrichtlinie „Allow-all“ lautet.

HTTPS (TLS) kann verwendet werden, um das Abhören oder Manipulieren des Netzwerkverkehrs zu verhindern. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden.

Abhilfe

Informationen zur Aktualisierung der Origin-Protokollrichtlinie, sodass für eine CloudFront Verbindung eine Verschlüsselung erforderlich ist, finden Sie im Amazon CloudFront Developer Guide unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung erforderlich machen.

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3),, NIST.800-53.r5 SC-12 (4) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (1), (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. PS-01.05, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-no-deprecated-ssl-protocols

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen veraltete SSL-Protokolle für die HTTPS-Kommunikation zwischen CloudFront Edge-Standorten und Ihren benutzerdefinierten Ursprüngen verwenden. Diese Kontrolle schlägt fehl, wenn eine CloudFront Distribution über ein Where Includes verfügt`CustomOriginConfig`. `OriginSslProtocols` `SSLv3`

Im Jahr 2015 gab die Internet Engineering Task Force (IETF) offiziell bekannt, dass SSL 3.0 nicht mehr unterstützt werden sollte, da das Protokoll nicht ausreichend sicher ist. Es wird empfohlen, dass Sie für die HTTPS-Kommunikation zu Ihren benutzerdefinierten Ursprüngen TLSv1.2 oder eine spätere Version verwenden.

Abhilfe

Informationen zur Aktualisierung der Origin-SSL-Protokolle für eine CloudFront Distribution finden Sie unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung erforderlich im Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

Verwandte Anforderungen: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0. 1/22.2.6, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-s3-origin-non-existent-bucket

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen auf nicht existierende Amazon S3-Ursprünge verweisen. Die Kontrolle schlägt bei einer CloudFront Distribution fehl, wenn der Ursprung so konfiguriert ist, dass er auf einen nicht existierenden Bucket verweist. Diese Steuerung gilt nur für CloudFront Distributionen, bei denen ein S3-Bucket ohne statisches Website-Hosting der S3-Ursprung ist.

Wenn eine CloudFront Distribution in Ihrem Konto so konfiguriert ist, dass sie auf einen nicht existierenden Bucket verweist, kann ein böswilliger Dritter den Bucket erstellen, auf den verwiesen wird, und seine eigenen Inhalte über Ihre Distribution bereitstellen. Wir empfehlen, alle Ursprünge unabhängig vom Routing-Verhalten zu überprüfen, um sicherzustellen, dass Ihre Distributionen auf die richtigen Ursprünge verweisen.

Abhilfe

Informationen zum Ändern einer CloudFront Distribution, sodass sie auf einen neuen Ursprung verweist, finden Sie unter Aktualisieren einer Distribution im Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-s3-origin-access-control-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für eine CloudFront Amazon-Distribution mit einem Amazon S3-Ursprung die Origin Access Control (OAC) konfiguriert ist. Die Kontrolle schlägt fehl, wenn OAC nicht für die CloudFront Distribution konfiguriert ist.

Wenn Sie einen S3-Bucket als Ursprung für Ihre CloudFront Distribution verwenden, können Sie OAC aktivieren. Dies ermöglicht den Zugriff auf den Inhalt im Bucket nur über die angegebene CloudFront Distribution und verhindert den direkten Zugriff aus dem Bucket oder einer anderen Distribution. Obwohl Origin Access Identity (OAI) CloudFront unterstützt wird, bietet OAC zusätzliche Funktionen, und Distributionen, die OAI verwenden, können zu OAC migriert werden. OAI bietet zwar eine sichere Möglichkeit, auf S3-Ursprünge zuzugreifen, weist jedoch Einschränkungen auf, z. B. mangelnde Unterstützung für detaillierte Richtlinienkonfigurationen und für HTTP/HTTPS Anfragen, die die POST-Methode verwenden und für die Signature Version 4 (Sigv4) erforderlich AWS ist. AWS-Regionen OAI unterstützt auch keine Verschlüsselung mit. AWS Key Management Service OAC basiert auf einer AWS bewährten Methode zur Verwendung von IAM-Dienstprinzipalen zur Authentifizierung mit S3-Ursprüngen.

Abhilfe

Informationen zur Konfiguration von OAC für eine CloudFront Distribution mit S3-Ursprüngen finden Sie unter Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung im Amazon CloudFront Developer Guide.

[CloudFront.14] CloudFront Distributionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config Regel: `tagged-cloudfront-distribution` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Distribution keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Verteilung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von

Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CloudFront Distribution finden Sie unter Tagging CloudFront Amazon-Distributionen im Amazon CloudFront Developer Guide.

[CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden

Verwandte Anforderungen: CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-ssl-policy-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:`securityPolicies`: `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025` (nicht anpassbar)

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution für die Verwendung einer empfohlenen TLS-Sicherheitsrichtlinie konfiguriert ist. Die Kontrolle schlägt fehl, wenn die CloudFront Distribution nicht für die Verwendung einer empfohlenen TLS-Sicherheitsrichtlinie konfiguriert ist.

Wenn Sie eine CloudFront Amazon-Distribution so konfigurieren, dass Zuschauer HTTPS für den Zugriff auf Inhalte verwenden müssen, müssen Sie eine Sicherheitsrichtlinie auswählen und die zu verwendende SSL/TLS Mindestprotokollversion angeben. Dies bestimmt, welche Protokollversion für die Kommunikation mit Zuschauern CloudFront verwendet wird und welche Chiffren zur Verschlüsselung der Kommunikation CloudFront verwendet werden. Wir empfehlen, die neueste Sicherheitsrichtlinie zu verwenden, die dies bietet. CloudFront Dadurch wird sichergestellt, dass die neuesten Cipher Suites CloudFront verwendet werden, um Daten zu verschlüsseln, die zwischen einem Viewer und einer Distribution übertragen werden. CloudFront

> **Note**
>
> Dieses Steuerelement generiert Ergebnisse nur für CloudFront Distributionen, die für die Verwendung benutzerdefinierter SSL-Zertifikate konfiguriert sind und die nicht für die Unterstützung älterer Clients konfiguriert sind.

Abhilfe

Informationen zur Konfiguration der Sicherheitsrichtlinie für eine CloudFront Distribution finden Sie unter Eine Distribution aktualisieren im Amazon CloudFront Developer Guide. Wenn Sie die Sicherheitsrichtlinie für eine Distribution konfigurieren, wählen Sie die neueste Sicherheitsrichtlinie aus.

[CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-origin-lambda-url-oac-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei einer CloudFront Amazon-Distribution mit einer AWS Lambda Funktions-URL als Ursprung die Origin Access Control (OAC) aktiviert ist. Die Steuerung schlägt fehl, wenn die CloudFront Distribution eine Lambda-Funktions-URL als Ursprung hat und OAC nicht aktiviert ist.

Eine AWS Lambda Funktions-URL ist ein dedizierter HTTPS-Endpunkt für eine Lambda-Funktion. Wenn eine Lambda-Funktions-URL der Ursprung einer CloudFront Distribution ist, muss die Funktions-URL öffentlich zugänglich sein. Aus Sicherheitsgründen sollten Sie daher ein OAC erstellen und es der Lambda-Funktions-URL in einer Distribution hinzufügen. OAC verwendet IAM-Dienstprinzipale, um Anfragen zwischen und der Funktions-URL zu authentifizieren. CloudFront Es unterstützt auch die Verwendung ressourcenbasierter Richtlinien, sodass der Aufruf einer Funktion nur dann zulässig ist, wenn eine Anfrage im Namen einer in der Richtlinie angegebenen Distribution erfolgt. CloudFront

Abhilfe

Informationen zur Konfiguration von OAC für eine CloudFront Amazon-Distribution, die eine Lambda-Funktions-URL als Ursprung verwendet, finden Sie unter Beschränken Sie den Zugriff auf einen AWS Lambda Funktions-URL-Ursprung im Amazon CloudFront Developer Guide.

[CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffskontrolle

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: cloudfront-distribution-key-group-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution so konfiguriert ist, dass sie vertrauenswürdige Schlüsselgruppen für die Authentifizierung mit signierten URLs oder signierten Cookies verwendet. Die Kontrolle schlägt fehl, wenn die CloudFront Distribution vertrauenswürdige Unterzeichner verwendet oder wenn für die Distribution keine Authentifizierung konfiguriert ist.

Um signierte URLs oder signierte Cookies verwenden zu können, benötigen Sie einen Aussteller. Ein Unterzeichner ist entweder eine vertrauenswürdige Schlüsselgruppe, in der Sie erstellen CloudFront, oder ein AWS Konto, das ein CloudFront key pair enthält. Wir empfehlen, vertrauenswürdige Schlüsselgruppen zu verwenden, da Sie bei CloudFront Schlüsselgruppen nicht den Root-Benutzer des AWS Kontos verwenden müssen, um die öffentlichen Schlüssel für CloudFront signierte URLs und signierte Cookies zu verwalten.

> **Note**
>
> Dieses Steuerelement bewertet keine CloudFront Distributionen (`connectionMode=tenant-only`) mit mehreren Mandanten.

Abhilfe

Informationen zur Verwendung vertrauenswürdiger Schlüsselgruppen mit signierten URLs und Cookies finden Sie unter Verwenden vertrauenswürdiger Schlüsselgruppen im Amazon CloudFront Developer Guide.

Security Hub CSPM-Steuerungen für AWS CloudTrail

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS CloudTrail Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.1, Benchmark für CIS AWS Foundations v1.2. 0/2.1, Benchmark für CIS AWS Foundations v1.4. 0/3.1, Benchmark für CIS AWS Foundations v3.0. 0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-14 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22), CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: multi-region-cloudtrail-enabled

Art des Zeitplans: Periodisch

Parameter:

- `readWriteType`: `ALL` (nicht anpassbar)

  `includeManagementEvents`: `true` (nicht anpassbar)

Dieses Steuerelement prüft, ob es mindestens einen multiregionalen AWS CloudTrail Trail gibt, der Lese- und Schreibverwaltungsereignisse erfasst. Das Steuerelement schlägt fehl, wenn es deaktiviert CloudTrail ist oder wenn es nicht mindestens einen CloudTrail Pfad gibt, der Lese- und Schreibverwaltungsereignisse erfasst.

AWS CloudTrail zeichnet AWS API-Aufrufe für Ihr Konto auf und übermittelt Ihnen Protokolldateien. Die aufgezeichneten Informationen umfassen die folgenden Informationen:

- Identität des API-Aufrufers
- Zeit des API-Aufrufs
- Quell-IP-Adresse des API-Aufrufers
- Anforderungsparameter
- Antwortelemente, die von zurückgegeben wurden AWS-Service

CloudTrail bietet eine Historie der AWS API-Aufrufe für ein Konto, einschließlich API-Aufrufen, die über die AWS SDKs AWS-Managementkonsole und Befehlszeilentools getätigt wurden. Der Verlauf umfasst auch API-Aufrufe von höheren Ebenen AWS-Services wie. AWS CloudFormation

Der von erstellte AWS API-Aufrufverlauf CloudTrail ermöglicht Sicherheitsanalysen, die Nachverfolgung von Ressourcenänderungen und die Überprüfung der Einhaltung von Vorschriften. Multi-Region Wanderwege bieten außerdem die folgenden Vorteile.

- Ein Multi-Regions-Trail hilft, unerwartete Aktivitäten zu erkennen, die in ansonsten nicht verwendeten Regionen auftreten.
- Ein Multi-Regions-Trail stellt sicher, dass Global Service Event Logging standardmäßig für einen Trail aktiviert ist. Die globale Protokollierung von Serviceereignissen zeichnet Ereignisse auf, die von AWS globalen Diensten generiert wurden.
- Bei einem Trail mit mehreren Regionen stellen Verwaltungsereignisse für alle Lese- und Schreibvorgänge sicher, dass die Verwaltungsvorgänge für alle Ressourcen in einem CloudTrail AWS-Konto aufgezeichnet werden.

Standardmäßig handelt es sich bei CloudTrail Pfaden, die mit dem AWS-Managementkonsole erstellt wurden, um Wanderwege mit mehreren Regionen.

Abhilfe

Informationen zum Erstellen eines neuen Wanderweges mit mehreren Regionen finden Sie unter Erstellen eines Wanderweges im AWS CloudTrail Benutzerhandbuch. CloudTrail Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Zusätzliche Einstellungen, Überprüfung der Protokolldatei	Aktiviert
Wählen Sie Protokollereignisse, Verwaltungsereignisse, API-Aktivität	Lesen und Schreiben. Deaktivieren Sie die Kontrollkästchen für Ausschlüsse.

Informationen zum Aktualisieren eines vorhandenen Pfads finden Sie unter Aktualisieren eines Pfads im AWS CloudTrail Benutzerhandbuch. Wählen Sie unter Verwaltungsereignisse für API-Aktivität die Optionen Lesen und Schreiben aus.

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.5, Benchmark für CIS AWS Foundations v1.2. 0/21.7, Benchmark für CIS AWS Foundations v1.4. 0/3.7, Benchmark v3.0 für CIS AWS Foundations. 0/3.5, NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/33.4, PCI DSS v4.0. 1/10.3.2, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: cloud-trail-encryption-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob CloudTrail es für die Verwendung der serverseitigen Verschlüsselung (SSE) AWS KMS key konfiguriert ist. Das Steuerelement schlägt fehl, wenn das `KmsKeyId` nicht definiert ist.

Für eine zusätzliche Sicherheitsebene für Ihre vertraulichen CloudTrail Protokolldateien sollten Sie die serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS) für Ihre CloudTrail Protokolldateien zur Verschlüsselung im Ruhezustand verwenden. Beachten Sie, dass die von an Ihre Buckets übermittelten Protokolldateien standardmäßig durch CloudTrail serverseitige Amazon-Verschlüsselung mit S3-managed Amazon-Verschlüsselungsschlüsseln () SSE-S3 verschlüsselt werden.

Abhilfe

Informationen zum Aktivieren der SSE-KMS Verschlüsselung für CloudTrail Protokolldateien finden Sie unter Aktualisieren eines Trails zur Verwendung eines KMS-Schlüssels im AWS CloudTrail Benutzerhandbuch.

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

Verwandte Anforderungen: NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/103.1, PCI DSS v3.2. 1/10.2.1, PCI DSS v3.2. 1/10.2.2, PCI DSS v3.2. 1/10.2.3, PCI-DSS v3.2. 1/10.2.4, PCI DSS v3.2. 1/10.2.5, PCI DSS v3.2. 1/10.2.6, PCI DSS v3.2. 1/10.2.7, PCI DSS v3.2. 1/10.3.1, PCI DSS v3.2. 1/10.3.2, PCI DSS v3.2. 1/10.3.3, PCI DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6, PCI DSS v4.0. 1/10.2.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: cloudtrail-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Steuerung prüft, ob in Ihrem ein AWS CloudTrail Trail aktiviert ist AWS-Konto. Die Kontrolle schlägt fehl, wenn für Ihr Konto nicht mindestens ein CloudTrail Trail aktiviert ist.

Einige AWS Dienste ermöglichen jedoch nicht die Protokollierung aller APIs und Ereignisse. Sie sollten alle zusätzlichen Prüfpfade einrichten, mit CloudTrail Ausnahme der Dokumentation der einzelnen Dienste CloudTrail unter Unterstützte Dienste und Integrationen.

Abhilfe

Informationen zu den ersten CloudTrail Schritten und zur Erstellung eines Trails finden Sie im AWS CloudTrail Tutorial Erste Schritte mit im AWS CloudTrail Benutzerhandbuch.

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.2, Benchmark für CIS AWS Foundations v1.2. 0/2.2, Benchmark für CIS AWS Foundations v1.4. 0/3.2, Benchmark v3.0 AWS für CIS Foundations. 0/3.2, NIST.800-53.r5 AU-9 NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), (3), NIST.800-53.r5 SI-7 NIST.800-53.r5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/105.5.2, PCI-DSS v3.2. 1/10.5.5, PCI DSS v4.0. 1/10.3.2, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Datenschutz > Datenintegrität

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: cloud-trail-log-file-validation-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft in einem CloudTrail Trail, ob die Integritätsprüfung der Protokolldatei aktiviert ist.

CloudTrail Bei der Überprüfung der Protokolldatei wird eine digital signierte Digest-Datei erstellt, die einen Hash jedes Protokolls enthält, das in Amazon S3 CloudTrail geschrieben wird. Sie können diese Digest-Dateien verwenden, um festzustellen, ob eine Protokolldatei nach CloudTrail der Übermittlung des Protokolls geändert, gelöscht oder unverändert wurde.

Security Hub CSPM empfiehlt, dass Sie die Dateiüberprüfung auf allen Wegen aktivieren. Die Protokolldateivalidierung bietet zusätzliche Integritätsprüfungen von CloudTrail Protokollen.

Abhilfe

Informationen zum Aktivieren der CloudTrail Protokolldateivalidierung finden Sie unter Aktivieren der Überprüfung der Integrität von AWS CloudTrail Protokolldateien CloudTrail im Benutzerhandbuch.

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/31.4, PCI DSS v3.2. 1/105.5.3, Benchmark für CIS AWS Foundations v1.2. 0/21.4, Benchmark für CIS AWS Foundations v1.4. 0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (1) NIST.800-53.r5 AU-3, (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), (20) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (5), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: cloud-trail-cloud-watch-logs-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Logs senden. Die Steuerung schlägt fehl, wenn die `CloudWatchLogsLogGroupArn` Eigenschaft des Trails leer ist.

CloudTrail zeichnet AWS API-Aufrufe auf, die in einem bestimmten Konto getätigt werden. Die aufgezeichneten Informationen umfassen Folgendes:

- Die Identität des API-Aufrufers
- Die Uhrzeit des API-Aufrufs
- Die Quell-IP-Adresse des API-Aufrufers
- Die Anforderungsparameter

- Die Antwortelemente, die von der zurückgegeben wurden AWS-Service

CloudTrail verwendet Amazon S3 für die Speicherung und Lieferung von Protokolldateien. Sie können CloudTrail Protokolle für langfristige Analysen in einem bestimmten S3-Bucket erfassen. Um Echtzeitanalysen durchzuführen, können Sie so konfigurieren, dass CloudWatch Protokolle CloudTrail an Logs gesendet werden.

CloudTrail Sendet bei einem Trail, der in allen Regionen eines Kontos aktiviert ist, Protokolldateien aus all diesen Regionen an eine CloudWatch Logs-Protokollgruppe.

Security Hub CSPM empfiehlt, dass Sie CloudTrail Protokolle an Logs senden CloudWatch . Beachten Sie, dass mit dieser Empfehlung sichergestellt werden soll, dass Kontoaktivitäten erfasst, überwacht und entsprechend alarmiert werden. Sie können CloudWatch Logs verwenden, um dies mit Ihrem AWS-Services einzurichten. Diese Empfehlung schließt die Verwendung einer anderen Lösung nicht aus.

Das Senden von CloudTrail CloudWatch Protokollen an Logs ermöglicht die Protokollierung von Aktivitäten in Echtzeit und im Verlauf auf der Grundlage von Benutzer, API, Ressource und IP-Adresse. Mit diesem Ansatz können Sie Alarme und Benachrichtigungen für ungewöhnliche oder sensible Kontoaktivitäten einrichten.

Abhilfe

Informationen zur Integration CloudTrail mit CloudWatch Logs finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse an CloudWatch Logs senden.

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/2.3, Benchmark für CIS AWS Foundations v1.4. 0/3.3, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Periodisch und durch Änderung ausgelöst

Parameter: Keine

CloudTrail protokolliert eine Aufzeichnung jedes API-Aufrufs, der in Ihrem Konto getätigt wurde. Diese Protokolldateien werden in einem S3-Bucket gespeichert. CIS empfiehlt, die S3-Bucket-Richtlinie oder Zugriffskontrollliste (ACL) auf den S3-Bucket anzuwenden, der CloudTrail protokolliert, um den öffentlichen Zugriff auf die CloudTrail Protokolle zu verhindern. Wenn der öffentliche Zugriff auf CloudTrail Protokollinhalte gewährt wird, kann dies einem Angreifer dabei helfen, Schwachstellen in der Nutzung oder Konfiguration des betroffenen Kontos zu erkennen.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM zunächst benutzerdefinierte Logik, um nach dem S3-Bucket zu suchen, in dem Ihre CloudTrail Logs gespeichert sind. Anschließend überprüft es anhand der AWS Config verwalteten Regeln, ob der Bucket öffentlich zugänglich ist.

Wenn Sie Ihre Logs in einem einzigen zentralen S3-Bucket zusammenfassen, führt Security Hub CSPM die Prüfung nur für das Konto und die Region durch, in der sich der zentrale S3-Bucket befindet. Für andere Konten und Regionen lautet der Kontrollstatus Keine Daten.

Wenn der Bucket öffentlich zugänglich ist, generiert die Prüfung einen Fehlschlag.

Abhilfe

Informationen zum Blockieren des öffentlichen Zugriffs auf Ihren CloudTrail S3-Bucket finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie alle vier Amazon S3 Block Public Access-Einstellungen aus.

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/2.6, Benchmark für CIS AWS Foundations v1.4. 0/3.6, Benchmark v3.0 für CIS AWS Foundations. 0/3.4, PCI DSS v4.0. 1/10.2.1, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Die S3-Bucket-Zugriffsprotokollierung generiert ein Protokoll, das Zugriffsdatensätze für jede Anfrage an Ihren S3-Bucket enthält. Ein Zugriffsprotokoll-Datensatz enthält Details über jede Anfrage, wie beispielsweise den Anforderungstyp, die in der Anfrage angeforderten Ressource sowie Uhrzeit und Datum der Anfrage.

CIS empfiehlt, die Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket zu aktivieren.

Durch das Aktivieren der S3-Bucket-Protokollierung für Ziel-S3-Buckets können Sie alle Ereignisse erfassen, die Auswirkungen auf Objekte in einem Ziel-Bucket haben können. Wenn Protokolle so konfiguriert sind, dass sie in einem separaten Bucket platziert werden, haben Sie Zugang zu Protokollinformationen, die in Sicherheits- und Vorfallreaktions-Workflows hilfreich sein können.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM zunächst benutzerdefinierte Logik, um nach dem Bucket zu suchen, in dem Ihre CloudTrail Protokolle gespeichert sind, und verwendet dann die AWS Config verwaltete Regel, um zu überprüfen, ob die Protokollierung aktiviert ist.

Wenn CloudTrail Protokolldateien von mehreren AWS-Konten in einen einzigen Amazon S3 S3-Ziel-Bucket übertragen werden, bewertet Security Hub CSPM diese Kontrolle nur anhand des Ziel-Buckets in der Region, in der er sich befindet. Dadurch werden Ihre Ergebnisse optimiert. Sie sollten diese Option jedoch CloudTrail in allen Konten aktivieren, die Protokolle an den Ziel-Bucket senden. Für alle Konten außer dem Konto, das den Ziel-Bucket enthält, lautet der Kontrollstatus Keine Daten.

Abhilfe

Informationen zum Aktivieren der Serverzugriffsprotokollierung für Ihren CloudTrail S3-Bucket finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung im Amazon Simple Storage Service-Benutzerhandbuch.

[CloudTrail.9] CloudTrail Pfade sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config Regel: `tagged-cloudtrail-trail` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS CloudTrail Trail Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Trail keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Trail mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudTrail Trail finden Sie AddTagsin der AWS CloudTrail API-Referenz.

[CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::CloudTrail::EventDataStore`

AWS Config -Regel: event-data-store-cmk-encryption-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`kmsKeyArns`	Eine Liste der Amazon-Ressourcennamen	StringList (maximal 3 Elemente)	1—3 ARNs vorhandener KMS-Schlü	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	(ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerelement generiert einen FAILED Befund, wenn ein Ereignisdatenspeicher nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.		ssel. Beispiel: arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab .	

Mit diesem Steuerelement wird geprüft, ob ein AWS CloudTrail Lake-Ereignisdatenspeicher im Ruhezustand verschlüsselt ist, wenn er vom Kunden verwaltet wird. AWS KMS key Die Steuerung schlägt fehl, wenn der Ereignisdatenspeicher nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

Standardmäßig verschlüsselt AWS CloudTrail Lake Ereignisdatenspeicher mithilfe eines AES-256 Algorithmus mit von Amazon S3 verwalteten Schlüsseln (SSE-S3). Für zusätzliche Kontrolle können Sie CloudTrail Lake so konfigurieren, dass stattdessen ein Ereignisdatenspeicher mit einem vom Kunden verwalteten AWS KMS key (SSE-KMS) verschlüsselt wird. Ein kundenverwalteter KMS-Schlüssel ist ein AWS KMS key Schlüssel, den Sie in Ihrem AWS-Konto erstellen, besitzen und verwalten. Sie haben die volle Kontrolle über diese Art von KMS-Schlüssel. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels. Sie können einen vom Kunden verwalteten KMS-Schlüssel für kryptografische Operationen für Ihre CloudTrail Daten verwenden und die Nutzung anhand von Protokollen überprüfen. CloudTrail

Abhilfe

Informationen zum Verschlüsseln eines AWS CloudTrail Lake-Ereignisdatenspeichers mit einem AWS KMS key von Ihnen angegebenen Datenspeicher finden Sie unter Aktualisieren eines Ereignisdatenspeichers im AWS CloudTrail Benutzerhandbuch. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

Security Hub CSPM-Steuerungen für Amazon CloudWatch

Diese AWS Security Hub CSPM Kontrollen bewerten den CloudWatch Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/1.1, Benchmark für CIS AWS Foundations v1.2. 0/3.3, Benchmark für CIS AWS Foundations v1.4. 0/11.7, Benchmark für CIS AWS Foundations v1.4. 0/41.3, NIST.800-171.r2 3.14.6, 3.14.7, PCI NIST.800-171.r2 DSS v3.2. 1/72.2.1, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Der Root-Benutzer hat uneingeschränkten Zugriff auf alle Dienste und Ressourcen in einem AWS-Konto. Wir empfehlen dringend, den Root-Benutzer nicht für tägliche Aufgaben zu verwenden. Durch die Minimierung der Nutzung des Root-Benutzers und die Anwendung des Prinzips der geringsten Rechte für die Zugriffsverwaltung wird das Risiko unbeabsichtigter Änderungen und der unbeabsichtigten Offenlegung hochberechtigter Anmeldeinformationen verringert.

Es hat sich bewährt, Ihre Root-Benutzeranmeldedaten nur dann zu verwenden, wenn sie für die Durchführung von Konto- und Dienstverwaltungsaufgaben erforderlich sind. Wenden Sie AWS Identity and Access Management (IAM-) Richtlinien direkt auf Gruppen und Rollen an, aber nicht auf Benutzer. Ein Tutorial zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 1.7 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse,

die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**

Feld	Value (Wert)
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm,AWS::CloudTrail::Trail, AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für nicht autorisierte API-Aufrufe zu erstellen. Die Überwachung nicht autorisierter API-Aufrufe hilft, Anwendungsfehler aufzudecken, und kann die Erkennung böswilliger Aktivitäten beschleunigen.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.1 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers

generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

[CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/32.2, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und Alarm-Konsolen-Logins zu erstellen, die nicht durch MFA geschützt sind. Durch die Überwachung zur Feststellung von Single-Factor-Konsolenanmeldungen wird die Transparenz im Hinblick auf Konten ohne MFA-Schutz gesteigert.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.2 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**

Feld	Value (Wert)
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.4, Benchmark für CIS AWS Foundations v1.4. 0/4.4, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm,AWS::CloudTrail::Trail, AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarme einrichtet.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an den IAM-Richtlinien zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-

Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

> **Note**
>
> Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die aus IAM-API-Aufrufen stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRo`

Feld	Value (Wert)
	`lePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/3.5, Benchmark für CIS AWS Foundations v1.4. 0/4.5, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den CloudTrail Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz für Aktivitäten in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.5 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich

um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/3.6, Benchmark für CIS AWS Foundations v1.4. 0/4.6, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für fehlgeschlagene Konsolenauthentifizierungsversuche zu erstellen. Durch die Überwachung fehlgeschlagenere Konsolenanmeldungen kann die Vorlaufzeit für die Erkennung von Brute-Force-Angriffsversuchen auf Anmeldeinformationen reduziert werden, durch die ein Indikator geliefert werden kann (wie z. B. eine Quell-IP), den Sie in anderen Ereigniskorrelationen verwenden können.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.6 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich

um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.7, Benchmark für CIS AWS Foundations v1.4. 0/4.7, NIST.800-171.r2 3.13.10, NIST.800-171.r2 3.13.16, 3.14.6, 3.14.7, CRI-Profil NIST.800-171.r2 v2. NIST.800-171.r2 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für vom Kunden verwaltete Schlüssel zu erstellen, deren Status in „Deaktiviert“ oder „Geplantes Löschen“ geändert wurde. Mit deaktivierten oder gelöschten Schlüsseln verschlüsselte Daten sind nicht mehr zugänglich.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.7 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden. Die Kontrolle schlägt auch fehl, wenn `ExcludeManagementEventSources` `kms.amazonaws.com`

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich

um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/3.8, Benchmark für CIS AWS Foundations v1.4. 0/4.8, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, dass Sie einen Metrikfilter und einen Alarm für Änderungen an den S3-Bucket-Richtlinien erstellen. Durch das Überwachen dieser Änderungen können Sie die Zeit reduzieren, die zum Erkennen und Korrigieren permissiver Richtlinien für sensible S3-Buckets erforderlich ist.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.8 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich

um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/3.9, Benchmark für CIS AWS Foundations v1.4. 0/4.9, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den AWS Config Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz im Hinblick auf Konfigurationselemente in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.9 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen

genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
> Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.
>
>   Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.
>
> Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-

Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.0, Benchmark für CIS AWS Foundations v1.4. 0/4.10, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-01.05, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Sicherheitsgruppen sind ein zustandsorientierter Paketfilter zur Steuerung von ein- und ausgehendem Datenverkehr in einer VPC.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an Sicherheitsgruppen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass -Ressourcen und -Services nicht unbeabsichtigt ungeschützt sind.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.10 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers

generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=AuthorizeSecurityGroupIngress) || ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) || ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) ||`

Feld	Value (Wert)
	`($.eventName=DeleteSecurity Group)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.1, Benchmark für CIS AWS Foundations v1.4. 0/4.11, NIST.800-171.r2 3.14.6, 3.14.7, NIST.800-171.r2 CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch NACLs dienen als zustandslose Paketfilter zur Steuerung von ein- und ausgehendem Datenverkehr für Subnetze in einer VPC.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an NACLs zu erstellen. Durch die Überwachung dieser Änderungen wird sichergestellt, dass AWS Ressourcen und Dienste nicht unbeabsichtigt offengelegt werden.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.11 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto

oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) ||`

Feld	Value (Wert)
	`($.eventName=DeleteNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclEntry) || ($.eventName=ReplaceNetworkAclAssociation)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.2, Benchmark für CIS AWS Foundations v1.4. 0/4.12, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:
`AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,
`AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Netzwerk-Gateways sind erforderlich, um Datenverkehr an ein Ziel außerhalb einer VPC zu senden und Datenverkehr von einem solchen Ziel zu empfangen.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an Netzwerk-Gateways zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass der gesamte eingehende und ausgehende Datenverkehr die VPC-Grenze über einen kontrollierten Pfad durchquert.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.12 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
> Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal
als...	**`1`**

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.3, Benchmark für CIS AWS Foundations v1.4. 0/4.13, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2

3.14.7, CRI-Profil v2. NIST.800-171.r2 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarme einrichtet. Routing-Tabellen leiten Netzwerkdatenverkehr zwischen Subnetzen und Netzwerk-Gateways weiter.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an Routentabellen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass sämtlicher VPC-Datenverkehr durch einen erwarteten Pfad fließt.

> **Note**
>
> Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
> Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

> **Note**
>
> Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die aus API-Aufrufen von Amazon Elastic Compute Cloud (EC2) stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.

2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Greater/Equal

Feld	Value (Wert)
als...	**1**

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/31.4, Benchmark für CIS AWS Foundations v1.4. 0/4.14, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7, CRI-Profil v2. NIST.800-171.r2 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: `AWS::Logs::MetricFilterAWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Sie können mehr als eine VPC in Ihrem Konto haben und eine Peer-Verbindung zwischen zwei VPCs erstellen, sodass Netzwerkdatenverkehr zwischen VPCs weitergeleitet werden kann.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an VPCs zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Um diese Prüfung durchzuführen, verwendet Security Hub CSPM eine benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.14 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub CSPM die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Multi-Region Wanderwege können sich auch in einer anderen Region befinden.
Die Prüfung führt zu `FAILED` Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Es hat sich bewährt, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub CSPM `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Metrischer Namespace	**`LogMetrics`**

Feld	Value (Wert)
Metrikwert	**1**
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Greater/Equal
als...	**1**

Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 IR-4 (5),, (12) NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.3.4, NIST.800-171.r2 3.14.6, CRI Profile v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::CloudWatch::Alarm`

AWS Config Regel: **`cloudwatch-alarm-action-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`alarmActionRequired`	Die Steuerung ermittelt, ob `PASSED` der Parameter auf eingestellt ist `true` und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechselt. `ALARM`	Boolesch	Nicht anpassbar	`true`
`insufficientDataActionRequired`	Die Steuerung ermittelt, `PASSED` ob der Parameter auf eingestellt ist `true` und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechselt`INSUFFICIENT_DATA` .	Boolesch	`true` oder `false`	`false`
`okActionRequired`	Die Steuerung gibt einen `PASSED` Befund aus, wenn der Parameter auf eingestellt ist `true` und der Alarm eine Aktion ausführt, wenn sich der Alarmstatus auf ändert`OK`.	Boolesch	`true` oder `false`	`false`

Dieses Steuerelement prüft, ob für einen CloudWatch Amazon-Alarm mindestens eine Aktion für den `ALARM` Status konfiguriert ist. Die Steuerung schlägt fehl, wenn für den Alarm keine Aktion für den `ALARM` Status konfiguriert ist. Optional können Sie benutzerdefinierte Parameterwerte angeben, sodass auch Alarmaktionen für die `OK` Zustände `INSUFFICIENT_DATA` oder erforderlich sind.

> **Note**
>
> Security Hub CSPM bewertet diese Kontrolle auf CloudWatch der Grundlage metrischer Alarme. Metrische Alarme können Teil von zusammengesetzten Alarmen sein, für die die

angegebenen Aktionen konfiguriert sind. Die Steuerung generiert `FAILED` Ergebnisse in den folgenden Fällen:

- Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
- Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den die angegebenen Aktionen konfiguriert sind.

Diese Steuerung konzentriert sich darauf, ob für einen CloudWatch Alarm eine Alarmaktion konfiguriert ist, wohingegen der Aktivierungsstatus einer CloudWatch Alarmaktion im CloudWatch.17Mittelpunkt steht.

Wir empfehlen CloudWatch Alarmaktionen, um Sie automatisch zu benachrichtigen, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Mithilfe von Überwachungsalarmen können Sie ungewöhnliche Aktivitäten erkennen und schnell auf Sicherheits- und Betriebsprobleme reagieren, wenn ein Alarm in einen bestimmten Zustand übergeht. Die häufigste Art von Alarmaktion besteht darin, einen oder mehrere Benutzer zu benachrichtigen, indem eine Nachricht an ein Amazon Simple Notification Service (Amazon SNS) -Thema gesendet wird.

Abhilfe

Informationen zu Aktionen, die von CloudWatch Alarmen unterstützt werden, finden Sie unter Alarmaktionen im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

Kategorie: Identifizieren > Protokollierung

Verwandte Anforderungen: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),, NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-12, CRI-Profil v2. 2/ID. AM-08.03, CRI-Profil v2. 2/ID. AM-08.05, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.03

Schweregrad: Mittel

Art der Ressource: `AWS::Logs::LogGroup`

AWS Config Regel: **`cw-loggroup-retention-period-check`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minRetentionTime`	Mindestaufbewahrungsdauer in Tagen für Protokollgruppen CloudWatch	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`

Diese Kontrolle prüft, ob eine CloudWatch Amazon-Protokollgruppe eine Aufbewahrungsfrist von mindestens der angegebenen Anzahl von Tagen hat. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsdauer unter der angegebenen Anzahl liegt. Sofern Sie keinen benutzerdefinierten Parameterwert für den Aufbewahrungszeitraum angeben, verwendet Security Hub CSPM einen Standardwert von 365 Tagen.

CloudWatch Logs zentralisieren die Logs all Ihrer Systeme und Anwendungen AWS-Services in einem einzigen, hoch skalierbaren Service. Sie können CloudWatch Logs verwenden, um Ihre Protokolldateien von Amazon Elastic Compute Cloud (EC2) -Instances, Amazon Route 53 und anderen Quellen zu überwachen AWS CloudTrail, zu speichern und darauf zuzugreifen. Wenn Sie Ihre Logs mindestens ein Jahr lang aufbewahren, können Sie die Standards für die Aufbewahrung von Protokollen einhalten.

Abhilfe

Informationen zur Konfiguration der Protokollaufbewahrungseinstellungen finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

Kategorie: Erkennung > Erkennungsservices

Verwandte Anforderungen: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12), CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01

Schweregrad: Hoch

Art der Ressource: `AWS::CloudWatch::Alarm`

AWS Config Regel: **`cloudwatch-alarm-action-enabled-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudWatch Alarmaktionen aktiviert sind (`ActionEnabled`sollte auf true gesetzt sein). Die Steuerung schlägt fehl, wenn die Alarmaktion für einen CloudWatch Alarm deaktiviert ist.

> **Note**
>
> Security Hub CSPM bewertet diese Kontrolle auf CloudWatch der Grundlage metrischer Alarme. Metrische Alarme können Teil von zusammengesetzten Alarmen sein, bei denen die Alarmaktionen aktiviert sind. Die Steuerung generiert `FAILED` Ergebnisse in den folgenden Fällen:
>
> - Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
> - Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den Alarmaktionen aktiviert sind.

Diese Steuerung konzentriert sich auf den Aktivierungsstatus einer CloudWatch Alarmaktion, während sie CloudWatch.15sich darauf konzentriert, ob eine `ALARM` Aktion in einem CloudWatch Alarm konfiguriert ist.

Alarmaktionen benachrichtigen Sie automatisch, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Wenn die Alarmaktion deaktiviert ist, werden keine Aktionen ausgeführt, wenn sich der Status des Alarms ändert, und Sie werden nicht über Änderungen der überwachten Messwerte informiert. Wir empfehlen, CloudWatch Alarmaktionen zu aktivieren, damit Sie schnell auf Sicherheits- und Betriebsprobleme reagieren können.

Abhilfe

Um eine CloudWatch Alarmaktion zu aktivieren (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich unter Alarme die Option Alle Alarme aus.
3. Wählen Sie den Alarm aus, für den Sie Aktionen aktivieren möchten.
4. Wählen Sie für Aktionen die Option Alarmaktionen — neu und dann Aktivieren aus.

Weitere Informationen zur Aktivierung von CloudWatch Alarmaktionen finden Sie unter Alarmaktionen im CloudWatch Amazon-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für CodeArtifact

Diese Security Hub CSPM-Steuerungen bewerten den AWS CodeArtifact Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeArtifact::Repository`

AWS ConfigRegel: `tagged-codeartifact-repository` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CodeArtifact Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CodeArtifact Repository finden Sie unter Markieren eines Repositorys CodeArtifact im AWS CodeArtifact Benutzerhandbuch.

Security Hub CSPM-Steuerungen für CodeBuild

Diese Security Hub CSPM-Steuerungen bewerten den AWS CodeBuild Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

Verwandte Anforderungen: NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. DS-02.01

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-source-repo-url-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die URL AWS CodeBuild des Bitbucket-Quell-Repositorys eines Projekts persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält. Die Kontrolle schlägt fehl, wenn die URL des Bitbucket-Quell-Repositorys persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.

> **Note**
>
> Dieses Steuerelement bewertet sowohl die Primärquelle als auch die Sekundärquellen eines CodeBuild Build-Projekts. Weitere Informationen zu Projektquellen finden Sie im AWS CodeBuild Benutzerhandbuch unter Beispiel für mehrere Eingabequellen und Ausgabeartefakte.

Sign-in Anmeldeinformationen sollten nicht im Klartext gespeichert oder übertragen werden oder in der Quell-Repository-URL erscheinen. Statt persönlicher Zugriffstoken oder Anmeldedaten solltest du auf deinen Quellanbieter zugreifen und deine Quell-Repository-URL so ändern CodeBuild, dass sie nur den Pfad zum Bitbucket-Repository-Speicherort enthält. Die Verwendung persönlicher Zugriffstoken oder Anmeldedaten könnte zu unbeabsichtigter Offenlegung von Daten oder unberechtigtem Zugriff führen.

Abhilfe

Sie können Ihr CodeBuild Projekt so aktualisieren, dass es OAuth verwendet.

Um das persönliche Zugriffstoken für die Standardauthentifizierung/(GitHub) aus CodeBuild der Projektquelle zu entfernen

1. Öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codebuild/.
2. Wählen Sie das Build-Projekt aus, das persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.
3. Wählen Sie unter Edit (Bearbeiten) die Option Source (Quelle) aus.
4. Wähle Disconnect from GitHub //Bitbucket aus.
5. Wähle Connect using OAuth und dann Connect to GitHub//Bitbucket.
6. Wenn Sie dazu aufgefordert werden, wählen Sie Autorisieren entsprechend aus.
7. Konfigurieren Sie Ihre Repository-URL und zusätzliche Konfigurationseinstellungen nach Bedarf neu.
8. Wählen Sie Update source (Quelle aktualisieren) aus.

Weitere Informationen findest du in den CodeBuild Anwendungsbeispielen im Benutzerhandbuch.AWS CodeBuild

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

Verwandte Anforderungen: NIST.800-53.r5 IA-5 (7) NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-06.04

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-envvar-awscred-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Projekt die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` enthält.

Die Anmeldeinformationen für die Authentifizierung `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` sollten niemals in Klartext gespeichert werden, da dies zu einer unbeabsichtigten Datenoffenlegung und unbefugtem Zugriff führen kann.

Abhilfe

Informationen zum Entfernen von Umgebungsvariablen aus einem CodeBuild Projekt finden Sie AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts. Stellen Sie sicher, dass nichts für Umgebungsvariablen ausgewählt ist.

Sie können Umgebungsvariablen mit sensiblen Werten im AWS Systems Manager Parameterspeicher speichern oder AWS Secrets Manager sie dann aus Ihrer Build-Spezifikation abrufen. Anweisungen finden Sie im AWS CodeBuild Benutzerhandbuch im Feld „Wichtig“ im Abschnitt „Umgebung“.

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/103.3.2, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-s3-logs-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob Amazon S3 S3-Protokolle für ein AWS CodeBuild Projekt verschlüsselt sind. Die Kontrolle schlägt fehl, wenn die Verschlüsselung für S3-Protokolle für ein CodeBuild Projekt deaktiviert ist.

Die Verschlüsselung von Daten im Ruhezustand ist eine empfohlene bewährte Methode, um Ihre Daten um eine Ebene der Zugriffsverwaltung zu erweitern. Durch die Verschlüsselung der Protokolle im Ruhezustand AWS wird das Risiko verringert, dass ein Benutzer, der sich nicht authentifiziert hat, auf die auf der Festplatte gespeicherten Daten zugreift. Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff nicht autorisierter Benutzer auf die Daten einzuschränken.

Abhilfe

Informationen zum Ändern der Verschlüsselungseinstellungen für CodeBuild Projekt-S3-Protokolle finden Sie AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts.

[CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (8), CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. IR-04.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CodeBuild Projektumgebung über mindestens eine Protokolloption verfügt, entweder für S3 oder ob CloudWatch Protokolle aktiviert sind. Dieses Steuerelement schlägt fehl, wenn in einer CodeBuild Projektumgebung nicht mindestens eine Protokolloption aktiviert ist.

Aus Sicherheitsgründen ist die Protokollierung eine wichtige Funktion, um future forensische Maßnahmen im Falle von Sicherheitsvorfällen zu ermöglichen. Die Korrelation von Anomalien in CodeBuild Projekten mit Bedrohungserkennungen kann das Vertrauen in die Genauigkeit dieser Bedrohungserkennungen erhöhen.

Abhilfe

Weitere Informationen zur Konfiguration der CodeBuild Projektprotokolleinstellungen finden Sie im Benutzerhandbuch unter Erstellen eines Build-Projekts (Konsole). CodeBuild

[CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::CodeBuild::ReportGroup`

AWS Config -Regel: `codebuild-report-group-encrypted-at-rest`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Testergebnisse einer AWS CodeBuild Berichtsgruppe, die in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportiert werden, im Ruhezustand verschlüsselt sind. Die Kontrolle schlägt fehl, wenn der Export der Berichtsgruppe im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Verschlüsselung des Exports von Berichtsgruppen nach S3 finden Sie unter Aktualisieren einer Berichtsgruppe im AWS CodeBuild Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Profiler CodeGuru

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen von Amazon CodeGuru Profiler.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden

Verwandte Anforderungen: CRI Profile v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config -Regel: `codeguruprofiler-profiling-group-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon CodeGuru Profiler-Profiling-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredKeyTags` Die Kontrolle schlägt fehl, wenn die Profiling-Gruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Profilerstellungsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS

Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CodeGuru Profiler-Profiling-Gruppe finden Sie unter Tagging Profiling Groups im Amazon CodeGuru Profiler-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon Reviewer CodeGuru

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen von Amazon CodeGuru Reviewer.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config -Regel: `codegurureviewer-repository-association-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon CodeGuru Reviewer-Repository-Zuordnung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Kontrolle schlägt fehl, wenn die Repository-Zuordnung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Repository-Zuordnung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS

Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CodeGuru Reviewer-Repository-Verknüpfung finden Sie unter Markieren einer Repository-Verknüpfung im Amazon CodeGuru Reviewer-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Cognito

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Cognito. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Ressourcentyp: `AWS::Cognito::UserPool`

AWS Config -Regel: cognito-user-pool-advanced-security-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`SecurityMode`	Der Modus zur Durchsetzung des Bedrohungsschutzes, nach dem das Steuerelement sucht.	Zeichenfolge	`AUDIT`, `ENFORCED`	`ENFORCED`

Diese Kontrolle prüft, ob in einem Amazon Cognito Cognito-Benutzerpool der Bedrohungsschutz aktiviert ist und der Erzwingungsmodus für die Standardauthentifizierung auf Vollfunktion eingestellt ist. Die Kontrolle schlägt fehl, wenn der Bedrohungsschutz für den Benutzerpool deaktiviert ist oder wenn der Erzwingungsmodus für die Standardauthentifizierung nicht auf volle Funktionalität eingestellt ist. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, verwendet Security Hub CSPM den Standardwert für den Erzwingungsmodus, der `ENFORCED` für die Standardauthentifizierung auf Vollfunktion gesetzt ist.

Nachdem Sie einen Amazon Cognito Cognito-Benutzerpool erstellt haben, können Sie den Bedrohungsschutz aktivieren und die Maßnahmen anpassen, die als Reaktion auf verschiedene Risiken ergriffen werden. Oder Sie können den Überwachungsmodus verwenden, um Metriken zu erkannten Risiken zu sammeln, ohne Sicherheitsmaßnahmen ergreifen zu müssen. Im Auditmodus veröffentlicht Threat Protection Kennzahlen an Amazon CloudWatch. Sie können Metriken sehen, nachdem Amazon Cognito sein erstes Ereignis generiert hat.

Abhilfe

Informationen zur Aktivierung des Bedrohungsschutzes für einen Amazon Cognito-Benutzerpool finden Sie unter Erweiterte Sicherheit mit Bedrohungsschutz im Amazon Cognito Developer Guide.

[Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-04.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::Cognito::IdentityPool`

AWS Config -Regel: cognito-identity-pool-unauth-access-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Cognito Cognito-Identitätspool so konfiguriert ist, dass er nicht authentifizierte Identitäten zulässt. Die Kontrolle schlägt fehl, wenn der Gastzugriff für den Identitätspool aktiviert ist (der `AllowUnauthenticatedIdentities` Parameter ist auf gesetzt`true`).

Wenn ein Amazon Cognito Cognito-Identitätspool nicht authentifizierte Identitäten zulässt, stellt der Identitätspool temporäre AWS Anmeldeinformationen für Benutzer bereit, die sich nicht über einen Identitätsanbieter authentifiziert haben (Gäste). Dies birgt Sicherheitsrisiken, da es anonymen Zugriff auf Ressourcen ermöglicht. AWS Wenn Sie den Gastzugriff deaktivieren, können Sie sicherstellen, dass nur ordnungsgemäß authentifizierte Benutzer auf Ihre AWS Ressourcen zugreifen können, wodurch das Risiko eines unbefugten Zugriffs und potenzieller Sicherheitsverletzungen verringert wird. Als bewährte Methode sollte ein Identitätspool die Authentifizierung durch unterstützte Identitätsanbieter erfordern. Wenn ein nicht authentifizierter Zugriff erforderlich ist, ist es wichtig, die Berechtigungen für nicht authentifizierte Identitäten sorgfältig einzuschränken und deren Verwendung regelmäßig zu überprüfen und zu überwachen.

Abhilfe

Informationen zur Deaktivierung des Gastzugriffs für einen Amazon Cognito-Identitätspool finden Sie unter Gastzugriff aktivieren oder deaktivieren im Amazon Cognito Developer Guide.

[Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben

Verwandte Anforderungen: CRI Profile v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::Cognito::UserPool`

AWS Config -Regel: cognito-user-pool-password-policy-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minLength`	Die Mindestanzahl an Zeichen, die ein Passwort enthalten muss.	Ganzzahl	8 auf 99	8

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requireLowercase`	Erfordert mindestens einen Kleinbuchstaben in einem Passwort.	Boolesch	`True`, `False`	`True`
`requireUppercase`	Erfordert mindestens einen Großbuchstaben in einem Passwort.	Boolesch	`True`, `False`	`True`
`requireNumbers`	Erfordert mindestens eine Zahl in einem Passwort.	Boolesch	`True`, `False`	`True`
`requireSymbols`	Erfordert mindestens ein Symbol in einem Passwort.	Boolesch	`True`, `False`	`True`
`temporaryPasswordValidity`	Die maximale Anzahl von Tagen, die ein Passwort bestehen kann, bevor es abläuft.	Ganzzahl	1 auf 365	7

Dieses Steuerelement prüft, ob die Passwortrichtlinie für einen Amazon Cognito Cognito-Benutzerpool die Verwendung sicherer Passwörter erfordert, basierend auf den empfohlenen Einstellungen für Passwortrichtlinien. Die Kontrolle schlägt fehl, wenn die Passwortrichtlinie für den Benutzerpool keine sicheren Passwörter erfordert. Sie können optional benutzerdefinierte Werte für die Richtlinieneinstellungen angeben, die das Steuerelement überprüft.

Starke Passwörter sind eine bewährte Sicherheitsmethode für Amazon Cognito Cognito-Benutzerpools. Schwache Passwörter können dazu führen, dass Benutzeranmeldedaten Systemen zugänglich gemacht werden, die Passwörter erraten und versuchen, auf Daten zuzugreifen. Dies gilt insbesondere für Anwendungen, die offen für das Internet sind. Passwortrichtlinien sind ein zentrales Element der Sicherheit von Benutzerverzeichnissen. Mithilfe einer Kennwortrichtlinie können Sie einen Benutzerpool so konfigurieren, dass er die Komplexität von Kennwörtern und andere Einstellungen erfordert, die Ihren Sicherheitsstandards und -anforderungen entsprechen.

Abhilfe

Informationen zum Erstellen oder Aktualisieren der Passwortrichtlinie für einen Amazon Cognito-Benutzerpool finden Sie unter Passwortanforderungen für Benutzerpools hinzufügen im Amazon Cognito Developer Guide.

[Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Ressourcentyp: `AWS::Cognito::UserPool`

AWS Config -Regel: cognito-userpool-cust-auth-threat-full-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob in einem Amazon Cognito Cognito-Benutzerpool der Bedrohungsschutz aktiviert ist und der Erzwingungsmodus für die benutzerdefinierte Authentifizierung auf Vollfunktion eingestellt ist. Die Kontrolle schlägt fehl, wenn für den Benutzerpool der Bedrohungsschutz deaktiviert ist oder wenn der Erzwingungsmodus für die benutzerdefinierte Authentifizierung nicht auf volle Funktionalität eingestellt ist.

Der Bedrohungsschutz, früher als erweiterte Sicherheitsfunktionen bezeichnet, besteht aus einer Reihe von Tools zur Überwachung unerwünschter Aktivitäten in Ihrem Benutzerpool sowie aus Konfigurationstools, mit denen potenziell bösartige Aktivitäten automatisch geschlossen werden. Nachdem Sie einen Amazon Cognito Cognito-Benutzerpool erstellt haben, können Sie den Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktivieren und die Maßnahmen anpassen, die als Reaktion auf verschiedene Risiken ergriffen werden. Full-function Der Modus umfasst eine Reihe von automatischen Reaktionen zur Erkennung unerwünschter Aktivitäten und kompromittierter Passwörter.

Abhilfe

Informationen zur Aktivierung des Bedrohungsschutzes für einen Amazon Cognito-Benutzerpool finden Sie unter Erweiterte Sicherheit mit Bedrohungsschutz im Amazon Cognito Developer Guide.

[Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein

Kategorie: Schützen > Sichere Zugriffsverwaltung > Authentifizierung Multi-factor

Schweregrad: Mittel

Art der Ressource: `AWS::Cognito::UserPool`

AWS Config -Regel: cognito-user-pool-mfa-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon Cognito Cognito-Benutzerpool, der mit einer Anmelderichtlinie nur mit Passwort konfiguriert ist, die Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Die Steuerung schlägt fehl, wenn für den Benutzerpool, der mit einer rein kennwortgeschützten Anmelderichtlinie konfiguriert ist, MFA nicht aktiviert ist.

Multi-factor Authentifizierung (MFA) fügt dem Faktor etwas, das Sie wissen, einen Authentifizierungsfaktor hinzu (normalerweise Benutzername und Passwort). Für Verbundbenutzer delegiert Amazon Cognito die Authentifizierung an den Identitätsanbieter (IdP) und bietet keine zusätzlichen Authentifizierungsfaktoren. Wenn Sie jedoch lokale Benutzer mit Kennwortauthentifizierung haben, erhöht die Konfiguration von MFA für den Benutzerpool deren Sicherheit.

> **Note**
>
> Diese Kontrolle gilt nicht für Verbundbenutzer und Benutzer, die sich mit kennwortlosen Faktoren anmelden.

Abhilfe

Informationen zur Konfiguration von MFA für einen Amazon Cognito-Benutzerpool finden Sie unter Hinzufügen von MFA zu einem Benutzerpool im Amazon Cognito Developer Guide.

[Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::Cognito::UserPool`

AWS Config -Regel: cognito-user-pool-deletion-protection-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon Cognito Cognito-Benutzerpool der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz für den Benutzerpool deaktiviert ist.

Durch den Löschschutz wird sichergestellt, dass Ihr Benutzerpool nicht versehentlich gelöscht wird. Wenn Sie einen Benutzerpool mit Löschschutz konfigurieren, kann der Pool von keinem Benutzer gelöscht werden. Der Löschschutz verhindert, dass Sie das Löschen eines Benutzerpools anfordern, es sei denn, Sie ändern den Pool zuerst und deaktivieren den Löschschutz.

Abhilfe

Informationen zum Konfigurieren des Löschschutzes für einen Amazon Cognito-Benutzerpool finden Sie unter Löschschutz für Benutzerpools im Amazon Cognito Developer Guide.

Security Hub CSPM-Steuerungen für AWS Config

Diese Security Hub CSPM-Steuerungen bewerten den AWS Config Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden

> **Note**
>
> Wenn Security Hub CSPM und Security Hub aktiviert sind, hat die Config.1 Regel immer den Status BESTANDEN. Dies liegt daran, dass Security Hub CSPM über einen serviceverknüpften Konfigurationsrekorder direkten Zugriff auf Konfigurationselemente hat. Der Parameter für dieses Steuerelement ist nicht anwendbar, da der interne serviceverknüpfte Konfigurationsrekorder automatisch mit der serviceverknüpften

Rolle erstellt wird. AWS Config Weitere Informationen finden Sie unter Verwenden des serviceverknüpften Konfigurationsrekorders.
Multicloud-Steuerelemente (wie Azure-Steuerelemente) und die damit verbundene Ressourcenaufzeichnung werden bei der Bewertung nicht berücksichtigt. Config.1 Multicloud-Standards verwenden immer einen internen serviceverknüpften Konfigurationsrekorder, den der CSPM-Multicloud-Connector unabhängig vom Aktivierungsstatus von Security Hub automatisch einrichtet. Da die Multicloud-Aufzeichnung vollständig vom Connector verwaltet wird, hat dies keinen Einfluss auf den Compliance-Status. Config.1 Config.1 bewertet nur die Konfiguration der AWS Ressourcenaufzeichnung.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.3, Benchmark für CIS AWS Foundations v1.2. 0/2.5, Benchmark für CIS AWS Foundations v1.4. 0/3.5, Benchmark v3.0 für CIS AWS Foundations. 0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1),, NIST.800-53.r5 CM-8 (2) NIST.800-53.r5 CM-8, PCI DSS v3.2. 1/105.5.2, PCI-DSS v3.2. 1/11.5, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Identifizieren > Bestand

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config Regel: Keine (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`includeConfigServiceLinkedRoleCheck`	Das Steuerelement bewertet nicht, ob die serviceverknüpfte Rolle AWS Config verwendet	Boolesch	`true` oder `false`	`true`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	wird, wenn der Parameter auf gesetzt ist. `false`			

Dieses Steuerelement prüft, ob AWS Config es in Ihrem Konto aktuell aktiviert ist AWS-Region, zeichnet alle Ressourcen auf, die den in der aktuellen Region aktivierten Kontrollen entsprechen, und verwendet die dienstverknüpfte Rolle AWS Config. Der Name der dienstbezogenen Rolle lautet. AWSServiceRoleForConfig Wenn Sie die dienstgebundene Rolle nicht verwenden und den `includeConfigServiceLinkedRoleCheck` Parameter nicht auf setzen, schlägt die Steuerung fehl`false`, da andere Rollen möglicherweise nicht über die erforderlichen Berechtigungen verfügen, AWS Config um Ihre Ressourcen korrekt aufzuzeichnen.

Der AWS Config Dienst führt die Konfigurationsverwaltung der unterstützten AWS Ressourcen in Ihrem Konto durch und übermittelt Ihnen Protokolldateien. Zu den aufgezeichneten Informationen gehören das Konfigurationselement (AWS Ressource), Beziehungen zwischen Konfigurationselementen und alle Konfigurationsänderungen innerhalb von Ressourcen. Globale Ressourcen sind Ressourcen, die in jeder Region verfügbar sind.

Die Kontrolle wird wie folgt bewertet:

- Wenn die aktuelle Region als Ihre Aggregationsregion festgelegt ist, liefert das Steuerelement nur `PASSED` Ergebnisse, wenn globale AWS Identity and Access Management (IAM-) Ressourcen aufgezeichnet werden (sofern Sie Steuerelemente aktiviert haben, für die diese erforderlich sind).
- Wenn die aktuelle Region als verknüpfte Region festgelegt ist, bewertet das Steuerelement nicht, ob globale IAM-Ressourcen aufgezeichnet wurden.
- Wenn die aktuelle Region nicht in Ihrem Aggregator enthalten ist oder wenn in Ihrem Konto keine regionsübergreifende Aggregation eingerichtet ist, liefert das Steuerelement nur dann `PASSED` Ergebnisse, wenn globale IAM-Ressourcen aufgezeichnet werden (sofern Sie Steuerelemente aktiviert haben, die diese erfordern).

Die Kontrollergebnisse werden nicht davon beeinflusst, ob Sie sich für die tägliche oder kontinuierliche Aufzeichnung von Änderungen des Ressourcenstatus in entscheiden. AWS Config Die Ergebnisse dieser Steuerung können sich jedoch ändern, wenn neue Steuerelemente veröffentlicht

werden, wenn Sie die automatische Aktivierung neuer Steuerelemente konfiguriert haben oder über eine zentrale Konfigurationsrichtlinie verfügen, die neue Kontrollen automatisch aktiviert. Wenn Sie in diesen Fällen nicht alle Ressourcen aufzeichnen, müssen Sie die Aufzeichnung für Ressourcen konfigurieren, die neuen Steuerelementen zugeordnet sind, um ein `PASSED` Ergebnis zu erhalten.

Security Hub CSPM-Sicherheitsprüfungen funktionieren nur dann wie vorgesehen, wenn Sie sie AWS Config in allen Regionen aktivieren und die Ressourcenaufzeichnung für Kontrollen konfigurieren, die dies erfordern.

> **Note**
>
> Config.1 erfordert, dass dies in allen Regionen aktiviert AWS Config ist, in denen Sie Security Hub CSPM verwenden.
> Da es sich bei Security Hub CSPM um einen regionalen Dienst handelt, wird bei der für dieses Steuerelement durchgeführten Prüfung nur die aktuelle Region für das Konto ausgewertet.
> Um Sicherheitsüberprüfungen anhand globaler IAM-Ressourcen in einer Region zuzulassen, müssen Sie globale IAM-Ressourcen in dieser Region aufzeichnen. Regionen, in denen keine globalen IAM-Ressourcen erfasst sind, erhalten eine `PASSED` Standardbewertung für Kontrollen, die globale IAM-Ressourcen überprüfen. Da globale IAM-Ressourcen überall identisch sind, empfehlen wir AWS-Regionen, globale IAM-Ressourcen nur in der Heimatregion aufzuzeichnen (sofern die regionsübergreifende Aggregation in Ihrem Konto aktiviert ist). IAM-Ressourcen werden nur in der Region aufgezeichnet, in der die globale Ressourcenaufzeichnung aktiviert ist.
> Die weltweit aufgezeichneten IAM-Ressourcentypen, die AWS Config unterstützt werden, sind IAM-Benutzer, Gruppen, Rollen und vom Kunden verwaltete Richtlinien. Sie können erwägen, Security Hub CSPM-Steuerelemente, die diese Ressourcentypen überprüfen, in Regionen zu deaktivieren, in denen die globale Ressourcenaufzeichnung deaktiviert ist.
> Weitere Informationen finden Sie unter Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM.

Abhilfe

Erfassen Sie in der Heimatregion und in Regionen, die nicht Teil eines Aggregators sind, alle Ressourcen, die für Kontrollen erforderlich sind, die in der aktuellen Region aktiviert sind, einschließlich globaler IAM-Ressourcen, falls Sie Steuerungen aktiviert haben, die globale IAM-Ressourcen erfordern.

In verknüpften Regionen können Sie einen beliebigen AWS Config Aufnahmemodus verwenden, sofern Sie alle Ressourcen aufzeichnen, die den Steuerelementen entsprechen, die in der aktuellen Region aktiviert sind. Wenn Sie in verknüpften Regionen Steuerelemente aktiviert haben, die die Aufzeichnung globaler IAM-Ressourcen erfordern, erhalten Sie kein `FAILED` Ergebnis (Ihre Aufzeichnung anderer Ressourcen ist ausreichend).

Anhand des `StatusReasons` Felds im `Compliance` Objekt Ihrer Suche können Sie feststellen, warum Sie für dieses Steuerelement einen Fehler gefunden haben. Weitere Informationen finden Sie unter Einzelheiten zur Einhaltung der Kontrollbestimmungen.

Eine Liste der Ressourcen, die für jedes Steuerelement aufgezeichnet werden müssen, finden Sie unterErforderlich AWS Config Ressourcen für Kontrollbefunde. Allgemeine Informationen zur Aktivierung AWS Config und Konfiguration der Ressourcenaufzeichnung finden Sie unterAktivierung und Konfiguration AWS Config für Security Hub CSPM.

Security Hub CSPM-Steuerungen für Amazon Connect

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen von Amazon Connect.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CustomerProfiles::ObjectType`

AWS Config -Regel: `customerprofiles-object-type-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Connect Connect-Objekttyp für Kundenprofile Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Objekttyp keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Objekttyp mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Objekttyp „Kundenprofile“ finden Sie unter Hinzufügen von Tags zu Ressourcen in Amazon Connect Customer im Connect-Kundenadministratorhandbuch.

[Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein

Verwandte Anforderungen: CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Connect::Instance`

AWS Config Regel: Connect-Instance-Logging aktiviert

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Connect Customer-Instance so konfiguriert ist, dass sie Flow-Logs generiert und in einer CloudWatch Amazon-Protokollgruppe speichert. Die Steuerung schlägt fehl, wenn die Connect Customer-Instanz nicht so konfiguriert ist, dass sie Flow-Logs generiert und in einer CloudWatch Protokollgruppe speichert.

Amazon Connect Connect-Kundenflussprotokolle bieten Echtzeitinformationen zu Ereignissen in Amazon Connect Connect-Kundenströmen. Ein Flow definiert das Kundenerlebnis mit einem Amazon Connect Connect-Kundenkontaktzentrum von Anfang bis Ende. Wenn Sie eine neue Amazon Connect Connect-Kundeninstanz erstellen, wird standardmäßig automatisch eine CloudWatch

Amazon-Protokollgruppe erstellt, um Flow-Logs für die Instance zu speichern. Mithilfe von Flow-Protokollen können Sie Abläufe analysieren, Fehler finden und Betriebskennzahlen überwachen. Sie können auch Benachrichtigungen für bestimmte Ereignisse einrichten, die in einem Flow auftreten können.

Abhilfe

Informationen zur Aktivierung von Flow-Protokollen für eine Amazon Connect Connect-Kundeninstanz finden Sie unter Amazon Connect Connect-Kundenflussprotokolle in einer CloudWatch Amazon-Protokollgruppe aktivieren im Connect-Kundenadministratorhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Data Firehose

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen von Amazon Data Firehose.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::KinesisFirehose::DeliveryStream`

AWS Config -Regel: `kinesis-firehose-delivery-stream-encrypted`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Data Firehose-Lieferstream im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt ist. Diese Steuerung schlägt fehl, wenn ein Firehose-Lieferstream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Server-side Verschlüsselung ist eine Funktion in Amazon Data Firehose-Lieferströmen, die Daten automatisch verschlüsselt, bevor sie gespeichert werden, indem ein in AWS Key Management

Service ()AWS KMS erstellter Schlüssel verwendet wird. Daten werden verschlüsselt, bevor sie in die Data Firehose-Stream-Speicherschicht geschrieben werden, und entschlüsselt, nachdem sie aus dem Speicher abgerufen werden. Auf diese Weise können Sie die gesetzlichen Anforderungen erfüllen und die Sicherheit Ihrer Daten verbessern.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Firehose-Lieferstreams finden Sie unter Datenschutz in Amazon Data Firehose im Amazon Data Firehose Developer Guide.

Security Hub CSPM-Steuerungen für AWS Database Migration Service

Diese AWS Security Hub CSPM Kontrollen bewerten die AWS Database Migration Service (AWS DMS) und AWS DMS Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config -Regel: dms-replication-not-public

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS DMS Replikationsinstanzen öffentlich sind. Zu diesem Zweck untersucht es den Wert des `PubliclyAccessible` Felds.

Eine private Replikationsinstanz hat eine private IP-Adresse, auf die Sie außerhalb des Replikationsnetzwerks nicht zugreifen können. Eine Replikationsinstanz sollte eine private IP-Adresse haben, wenn sich die Quell- und Zieldatenbank im selben Netzwerk befinden. Das Netzwerk muss auch über ein VPN oder VPC-Peering mit der VPC der Replikationsinstanz verbunden sein. Direct ConnectWeitere Informationen zu öffentlichen und privaten Replikationsinstanzen finden Sie im Benutzerhandbuch unter Öffentliche und private Replikationsinstanzen.AWS Database Migration Service

Sie sollten außerdem sicherstellen, dass der Zugriff auf Ihre AWS DMS Instanzkonfiguration nur autorisierten Benutzern vorbehalten ist. Beschränken Sie dazu die IAM-Berechtigungen der Benutzer, AWS DMS Einstellungen und Ressourcen zu ändern.

Abhilfe

Sie können die Einstellung für den öffentlichen Zugriff für eine DMS-Replikationsinstanz nicht ändern, nachdem Sie sie erstellt haben. Um die Einstellung für den öffentlichen Zugriff zu ändern, löschen Sie Ihre aktuelle Instanz und erstellen Sie sie anschließend neu. Wählen Sie nicht die Option Öffentlich zugänglich aus.

[DMS.2] DMS-Zertifikate sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::Certificate`

AWS Config Regel: `tagged-dms-certificate` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AWS DMS Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Zertifikat finden Sie unter Ressourcen kennzeichnen AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

[DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::EventSubscription`

AWS Config Regel: `tagged-dms-eventsubscription` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS DMS Ereignisabonnement Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Ereignisabonnement keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt

fehl, wenn das Ereignisabonnement mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Veranstaltungsabonnement finden Sie AWS Database Migration Service im Benutzerhandbuch unter Ressourcen taggen.AWS Database Migration Service

[DMS.4] DMS-Replikationsinstanzen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config Regel: `tagged-dms-replicationinstance` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine AWS DMS Replikationsinstanz über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Replikationsinstanz keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Replikationsinstanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationsinstanz finden Sie unter Ressourcen taggen AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

[DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::ReplicationSubnetGroup`

AWS Config Regel: `tagged-dms-replicationsubnetgroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß-	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	und Kleinschreibung unterschieden.			

Dieses Steuerelement prüft, ob eine AWS DMS Replikationssubnetzgruppe über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Replikationssubnetzgruppe keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Replikationssubnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationssubnetzgruppe finden Sie unter Ressourcen kennzeichnen im AWS Database Migration Service Benutzerhandbuch.AWS Database Migration Service

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config -Regel: dms-auto-minor-version-upgrade-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das automatische Upgrade einer Nebenversion für eine AWS DMS Replikationsinstanz aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für eine DMS-Replikationsinstanz nicht aktiviert ist.

DMS bietet ein automatisches Upgrade der Nebenversionen für jede unterstützte Replikationsengine, sodass Sie Ihre Replikationsinstanz auf dem neuesten Stand halten können. Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung des automatischen Upgrades für kleinere Versionen auf DMS-Replikationsinstanzen werden kleinere Upgrades automatisch während des Wartungsfensters oder sofort angewendet, wenn die Option Änderungen sofort anwenden ausgewählt ist.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades für Nebenversionen auf DMS-Replikationsinstanzen finden Sie unter Ändern einer Replikationsinstanz im AWS Database Migration Service Benutzerhandbuch.

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationTask`

AWS Config -Regel: dms-replication-task-targetdb-logging

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `TARGET_APPLY` und `TARGET_LOAD` aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch , um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `TARGET_APPLY` – Daten und Data Definition Language (DDL)-Anweisungen werden auf die Zieldatenbank angewendet.
- `TARGET_LOAD` – Daten werden in die Zieldatenbank geladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Problembehandlung, Prüfung, Leistungsanalyse, Fehlererkennung und -wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung

selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern Support.
Eine minimale Protokollierungsebene von `DEFAULT` stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement prüft, ob für die vorangegangenen Replikationsaufgaben mindestens eine der folgenden Protokollierungsstufen gilt: `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, oder`LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Zieldatenbank finden Sie unter AWS DMS Task-Logs anzeigen und verwalten im AWS Database Migration Service Benutzerhandbuch.

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationTask`

AWS Config -Regel: dms-replication-task-sourcedb-logging

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `SOURCE_CAPTURE` und `SOURCE_UNLOAD` aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch , um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `SOURCE_CAPTURE`— Laufende Replikations- oder CDC-Daten (Change Data Capture) werden aus der Quelldatenbank oder dem Quelldienst erfasst und an die `SORTER` Servicekomponente weitergegeben.
- `SOURCE_UNLOAD`— Daten werden bei Volllast aus der Quelldatenbank oder dem Quelldienst entladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Fehlerbehebung, Prüfung, Leistungsanalyse, Fehlererkennung und Wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern Support. Eine minimale Protokollierungsebene von `DEFAULT` stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement prüft, ob für die vorangegangenen Replikationsaufgaben mindestens eine der folgenden Protokollierungsstufen gilt: `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, oder`LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Quelldatenbank finden Sie unter AWS DMS Task-Logs anzeigen und verwalten im AWS Database Migration Service Benutzerhandbuch.

[DMS.9] DMS-Endpunkte sollten SSL verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4,, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: dms-endpoint-ssl-configured

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt eine SSL-Verbindung verwendet. Die Steuerung schlägt fehl, wenn der Endpunkt kein SSL verwendet.

SSL/TLS Verbindungen bieten eine Sicherheitsebene, indem sie Verbindungen zwischen DMS-Replikationsinstanzen und Ihrer Datenbank verschlüsseln. Die Verwendung von Zertifikaten bietet eine zusätzliche Sicherheitsebene, da überprüft wird, ob die Verbindung zur erwarteten Datenbank hergestellt wird. Dazu wird das Serverzertifikat überprüft, das automatisch auf allen von Ihnen bereitgestellten Datenbankinstanzen installiert wird. Durch die Aktivierung der SSL-Verbindung auf Ihren DMS-Endpunkten schützen Sie die Vertraulichkeit der Daten während der Migration.

Abhilfe

Informationen zum Hinzufügen einer SSL-Verbindung zu einem neuen oder vorhandenen DMS-Endpunkt finden Sie unter SSL verwenden mit AWS Database Migration Service im AWS Database Migration Service Benutzerhandbuch.

[DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2,,,, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-17, PCI DSS v4.0 NIST.800-53.r5 IA-2. NIST.800-53.r5 IA-5 1/73.3.1, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: dms-neptune-iam-authorization-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für eine Amazon Neptune Neptune-Datenbank mit IAM-Autorisierung konfiguriert ist. Die Kontrolle schlägt fehl, wenn für den DMS-Endpunkt keine IAM-Autorisierung aktiviert ist.

AWS Identity and Access Management (IAM) bietet eine differenzierte Zugriffskontrolle für alle Bereiche. AWS Mit IAM können Sie festlegen, wer unter welchen Bedingungen auf welche Dienste und Ressourcen zugreifen kann. Mit IAM-Richtlinien verwalten Sie die Berechtigungen für Ihre Mitarbeiter und Systeme, um sicherzustellen, dass die Berechtigungen mit den geringsten Rechten eingehalten werden. Indem Sie die IAM-Autorisierung auf AWS DMS Endpunkten für Neptune-Datenbanken aktivieren, können Sie IAM-Benutzern Autorisierungsprivilegien gewähren, indem Sie eine durch den Parameter angegebene Servicerolle verwenden. `ServiceAccessRoleARN`

Abhilfe

Informationen zur Aktivierung der IAM-Autorisierung auf DMS-Endpunkten für Neptune-Datenbanken finden Sie unter Verwenden von Amazon Neptune als Ziel für im Benutzerhandbuch. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-6 NIST.800-53.r5 IA-2, PCI DSS NIST.800-53.r5 IA-5 v4.0. 1/73.3.1, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: dms-mongo-db-authentication-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für MongoDB mit einem Authentifizierungsmechanismus konfiguriert ist. Die Steuerung schlägt fehl, wenn kein Authentifizierungstyp für den Endpunkt festgelegt ist.

AWS Database Migration Service unterstützt zwei Authentifizierungsmethoden für MongoDB — MONGODB-CRfür MongoDB Version 2.x und SCRAM-SHA-1für MongoDB Version 3.x oder höher. Diese Authentifizierungsmethoden werden verwendet, um MongoDB-Passwörter zu authentifizieren und zu verschlüsseln, wenn Benutzer die Passwörter für den Zugriff auf die Datenbanken verwenden möchten. Durch die Authentifizierung auf AWS DMS Endpunkten wird sichergestellt, dass nur autorisierte Benutzer auf die Daten zugreifen und diese ändern können, die zwischen Datenbanken migriert werden. Ohne ordnungsgemäße Authentifizierung können unbefugte Benutzer während des Migrationsprozesses möglicherweise auf sensible Daten zugreifen. Dies kann zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen.

Abhilfe

Informationen zur Aktivierung eines Authentifizierungsmechanismus auf DMS-Endpunkten für MongoDB finden Sie unter Verwenden von MongoDB als Quelle für AWS DMS im Benutzerhandbuch.AWS Database Migration Service

[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SC-8,, PCI DSS NIST.800-53.r5 SC-13 v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: dms-redis-tls-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für Redis OSS mit einer TLS-Verbindung konfiguriert ist. Die Steuerung schlägt fehl, wenn auf dem Endpunkt TLS nicht aktiviert ist.

TLS bietet umfassende Sicherheit, wenn Daten zwischen Anwendungen oder Datenbanken über das Internet gesendet werden. Wenn Sie die SSL-Verschlüsselung für Ihren DMS-Endpunkt konfigurieren, ermöglicht sie die verschlüsselte Kommunikation zwischen der Quell- und der Zieldatenbank während des Migrationsprozesses. Dies trägt dazu bei, das Abhören und Abfangen

sensibler Daten durch böswillige Akteure zu verhindern. Ohne SSL-Verschlüsselung kann auf sensible Daten zugegriffen werden, was zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen kann.

Abhilfe

Informationen zum Aktivieren einer TLS-Verbindung auf DMS-Endpunkten für Redis finden Sie unter Verwenden von Redis als Ziel für AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

[DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config -Regel: dms-replication-instance-multi-az-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS Database Migration Service (AWS DMS) Replikationsinstanz für die Verwendung mehrerer Availability Zones konfiguriert ist (Multi-AZ Bereitstellung). Die Steuerung schlägt fehl, wenn die AWS DMS Replikationsinstanz nicht für die Verwendung einer Multi-AZ Bereitstellung konfiguriert ist.

In einer Multi-AZ Bereitstellung AWS DMS wird automatisch ein Standby-Replikat einer Replikationsinstanz in einer anderen Availability Zone (AZ) bereitgestellt und verwaltet. Die primäre Replikationsinstanz wird dann synchron auf das Standby-Replikat repliziert. Wenn die primäre Replikations-Instance ausfällt oder nicht mehr reagiert, nimmt der Standby-Modus alle laufenden Tasks mit minimaler Unterbrechung wieder auf. Weitere Informationen finden Sie unter Arbeiten mit einer Replikationsinstanz im AWS Database Migration Service Benutzerhandbuch.

Abhilfe

Nachdem Sie eine AWS DMS Replikationsinstanz erstellt haben, können Sie die Multi-AZ Bereitstellungseinstellung für sie ändern. Informationen zum Ändern dieser und anderer Einstellungen

für eine bestehende Replikationsinstanz finden Sie unter Ändern einer Replikationsinstanz im AWS Database Migration Service Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS DataSync

Diese Security Hub CSPM-Steuerungen bewerten den AWS DataSync Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::DataSync::Task`

AWS Config -Regel: datasync-task-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS DataSync Aufgabe die Protokollierung aktiviert ist. Das Steuerelement schlägt fehl, wenn für die Aufgabe die Protokollierung nicht aktiviert ist.

In Auditprotokollen werden Systemaktivitäten verfolgt und überwacht. Sie bieten eine Aufzeichnung von Ereignissen, anhand derer Sie Sicherheitsverletzungen erkennen, Vorfälle untersuchen und Vorschriften einhalten können. Auditprotokolle verbessern auch die allgemeine Rechenschaftspflicht und Transparenz Ihres Unternehmens.

Abhilfe

Informationen zur Konfiguration der Protokollierung für AWS DataSync Aufgaben finden Sie unter Überwachen von Datenübertragungen mit Amazon CloudWatch Logs im AWS DataSync Benutzerhandbuch.

[DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden

Verwandte Anforderungen: CRI Profile v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DataSync::Task`

AWS Config -Regel: datasync-task-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS DataSync Aufgabe über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die Aufgabe über keine Tagschlüssel oder nicht über alle im `requiredKeyTags` Parameter angegebenen Schlüssel verfügt. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Aufgabe keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können

Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer AWS DataSync Aufgabe finden Sie unter Taggen Ihrer AWS DataSync Aufgaben im AWS DataSync Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon Detective

Diese AWS Security Hub CSPM Kontrolle bewertet den Service und die Ressourcen von Amazon Detective. Das Steuerelement ist möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Detective::Graph`

AWS ConfigRegel: `tagged-detective-graph` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Detective-Verhaltensdiagramm Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Verhaltensdiagramm keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Verhaltensdiagramm mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Verhaltensdiagramm von Detective finden Sie unter Hinzufügen von Tags zu einem Verhaltensdiagramm im Amazon Detective Administration Guide.

Security Hub CSPM-Steuerelemente für Amazon DocumentDB

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon DocumentDB (mit MongoDB-Kompatibilität). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: docdb-cluster-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DocumentDB-Cluster im Ruhezustand verschlüsselt ist. Die Kontrolle schlägt fehl, wenn ein Amazon DocumentDB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Amazon DocumentDB-Clustern sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten. Amazon DocumentDB verwendet den 256-Bit-Advanced Encryption Standard (AES-256), um Ihre Daten mit den in () gespeicherten Verschlüsselungsschlüsseln zu verschlüsseln. AWS Key Management Service AWS KMS

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Amazon DocumentDB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter Enabling at rest encryption for a Amazon DocumentDB cluster im Amazon DocumentDB Developer Guide.

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

Verwandte Anforderungen: NIST.800-53.r5 SI-12, PCI DSS v4.0. 1/32.2.1, CRI-Profil v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: docdb-cluster-backup-retention-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`minimumBackupRetentionPeriod`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster eine Aufbewahrungsdauer für Backups hat, die größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsfrist für Backups den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub CSPM einen Standardwert von 7 Tagen.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen und die Widerstandsfähigkeit Ihrer Systeme stärken. Durch die Automatisierung von Backups für Ihre Amazon DocumentDB-Cluster können Sie Ihre Systeme zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren. In Amazon DocumentDB haben Cluster eine standardmäßige Aufbewahrungsfrist für Backups von einem Tag. Dieser Wert muss auf einen Wert zwischen 7 und 35 Tagen erhöht werden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Ändern der Aufbewahrungsdauer von Backups für Ihre Amazon DocumentDB-Cluster finden Sie unter Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Wählen Sie für Backup den Aufbewahrungszeitraum für Backups aus.

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config -Regel: docdb-cluster-snapshot-public-prohibited

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Amazon DocumentDB-Cluster-Snapshot öffentlich ist. Die Kontrolle schlägt fehl, wenn der manuelle Cluster-Snapshot öffentlich ist.

Ein manueller Amazon DocumentDB-Cluster-Snapshot sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-KontenÖffentliche Snapshots können zu einer unbeabsichtigten Offenlegung von Daten führen.

> **Note**
>
> Dieses Steuerelement wertet manuelle Cluster-Snapshots aus. Sie können keinen automatisierten Amazon DocumentDB-Cluster-Snapshot teilen. Sie können jedoch einen manuellen Snapshot erstellen, indem Sie den automatisierten Snapshot kopieren und die Kopie dann teilen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Cluster-Snapshots von Amazon DocumentDB finden Sie unter Einen Snapshot teilen im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Programmgesteuert können Sie den Amazon DocumentDB DocumentDB-Vorgang verwenden. `modify-db-snapshot-attribute` Stellen Sie `attribute-name` als und als ein. `restore` `values-to-remove` `all`

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5

AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/103.3.3, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: docdb-cluster-audit-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn der Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch

Amazon DocumentDB (mit MongoDB-Kompatibilität) ermöglicht es Ihnen, Ereignisse zu überprüfen, die in Ihrem Cluster durchgeführt wurden. Beispiele für protokollierte Ereignisse sind erfolgreiche und fehlgeschlagene Authentifizierungsversuche, Drop-Ereignisse für Sammlungen in einer Datenbank oder das Erstellen eines Index. Standardmäßig ist die Prüfung in Amazon DocumentDB deaktiviert und erfordert, dass Sie Maßnahmen ergreifen, um sie zu aktivieren.

Abhilfe

Informationen zum Veröffentlichen von Amazon DocumentDB-Prüfprotokollen in CloudWatch Logs finden Sie unter Enabling Auditing im Amazon DocumentDB Developer Guide.

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: docdb-cluster-deletion-protection-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon DocumentDB-Cluster der Löschschutz aktiviert ist. Die Kontrolle schlägt fehl, wenn für den Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet einen zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Amazon DocumentDB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann. Der Löschschutz ist standardmäßig aktiviert, wenn Sie einen Cluster in der Amazon DocumentDB DocumentDB-Konsole erstellen.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Amazon DocumentDB-Cluster finden Sie unter Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Wählen Sie im Abschnitt „Cluster modifizieren“ die Option „Für den Löschschutz aktivieren“.

[DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: docdb-cluster-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter**`excludeTlsParameters`**:`disabled`, `enabled` (nicht anpassbar)

Diese Steuerung prüft, ob ein Amazon DocumentDB-Cluster TLS für Verbindungen zum Cluster benötigt. Die Steuerung schlägt fehl, wenn die dem Cluster zugeordnete Cluster-Parametergruppe nicht synchronisiert ist oder der TLS-Cluster-Parameter auf `disabled` oder `enabled` gesetzt ist.

Sie können TLS verwenden, um die Verbindung zwischen einer Anwendung und einem Amazon DocumentDB-Cluster zu verschlüsseln. Die Verwendung von TLS kann dazu beitragen, Daten davor zu schützen, dass sie abgefangen werden, während die Daten zwischen einer Anwendung und einem Amazon DocumentDB-Cluster übertragen werden. Die Verschlüsselung während der Übertragung für einen Amazon DocumentDB-Cluster wird mithilfe des TLS-Parameters in der Cluster-Parametergruppe verwaltet, die dem Cluster zugeordnet ist. Wenn die Verschlüsselung während der Übertragung aktiviert ist, sind sichere Verbindungen mit TLS erforderlich, um eine Verbindung mit dem Cluster herzustellen. Wir empfehlen die Verwendung der folgenden TLS-Parameter: `tls1.2+tls1.3+`, und`fips-140-3`.

Abhilfe

Informationen zum Ändern der TLS-Einstellungen für einen Amazon DocumentDB-Cluster finden Sie unter Verschlüsseln von Daten bei der Übertragung im Amazon DocumentDB Developer Guide.

Security Hub CSPM-Steuerelemente für DynamoDB

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon DynamoDB. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config -Regel: `dynamodb-autoscaling-enabled`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Gültige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minProvisionedReadCapacity`	Mindestanzahl bereitgestellter Lesekapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf `40000`	Kein Standardwert
`targetReadUtilization`	Zielauslastung in Prozent für die Lesekapazität	Ganzzahl	`20` auf `90`	Kein Standardwert
`minProvisionedWriteCapacity`	Mindestanzahl bereitgestellter Schreibkapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf `40000`	Kein Standardwert
`targetWriteUtilization`	Zielauslastung in Prozent für die Schreibkapazität	Ganzzahl	`20` auf `90`	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle ihre Lese- und Schreibkapazität nach Bedarf skalieren kann. Die Steuerung schlägt fehl, wenn die Tabelle nicht den On-Demand-Kapazitätsmodus oder den Bereitstellungsmodus mit konfigurierter Autoskalierung verwendet. Standardmäßig erfordert dieses Steuerelement nur, dass einer dieser Modi konfiguriert ist, unabhängig von bestimmten Lese- oder Schreibkapazitätsstufen. Optional können Sie benutzerdefinierte Parameterwerte angeben, um bestimmte Lese- und Schreibkapazitäten oder eine bestimmte Zielauslastung zu erfordern.

Durch die bedarfsgerechte Skalierung der Kapazität werden Drosselungen von Ausnahmen vermieden, wodurch die Verfügbarkeit Ihrer Anwendungen aufrechterhalten wird. DynamoDB-Tabellen, die den On-Demand-Kapazitätsmodus verwenden, sind nur durch die standardmäßigen Tabellenkontingente für den DynamoDB-Durchsatz begrenzt. Um diese Kontingente zu erhöhen, können Sie ein Supportticket bei einreichen. Support DynamoDB-Tabellen, die den Bereitstellungsmodus mit Auto Scaling verwenden, passen die bereitgestellte Durchsatzkapazität dynamisch an Verkehrsmuster an. Weitere Informationen zur DynamoDB-Anforderungsdrosselung

finden Sie unter Anforderungsdrosselung und Burstkapazität im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Abhilfe

Informationen zur Aktivierung der automatischen DynamoDB-Skalierung für bestehende Tabellen im Kapazitätsmodus finden Sie unter Aktivieren der auto Skalierung von DynamoDB für bestehende Tabellen im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Point-in-Time-Wiederherstellung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9,, NIST.800-53.r5 SC-5 NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::DynamoDB::Table`

AWS Config -Regel: `dynamodb-pitr-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Point-in-Time Recovery (PITR) für eine Amazon DynamoDB-Tabelle aktiviert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. DynamoDB Point-in-Time-Recovery automatisiert Backups für DynamoDB-Tabellen. Dadurch wird die Zeit für die Wiederherstellung nach versehentlichen Lösch- oder Schreibvorgängen reduziert. DynamoDB-Tabellen, für die PITR aktiviert ist, können zu einem beliebigen Zeitpunkt der letzten 35 Tage wiederhergestellt werden.

Abhilfe

Informationen zum Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt finden Sie unter Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::DAX::Cluster`

AWS Config -Regel: `dax-encryption-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DynamoDB Accelerator (DAX) -Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der DAX-Cluster im Ruhezustand nicht verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den keine Authentifizierung angemeldet ist. AWS Durch die Verschlüsselung werden weitere Zugriffskontrollen hinzugefügt, um den Zugriff nicht autorisierter Benutzer auf die Daten zu beschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand nicht aktivieren oder deaktivieren, nachdem ein Cluster erstellt wurde. Sie müssen den Cluster neu erstellen, um die Verschlüsselung im Ruhezustand zu aktivieren. Ausführliche Anweisungen zum Erstellen eines DAX-Clusters mit aktivierter Verschlüsselung im Ruhezustand finden Sie unter Enabling at rest using the AWS-Managementkonsole im Amazon DynamoDB Developer Guide.

[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::DynamoDB::Table`

AWS Config Regel: **`dynamodb-resources-protected-by-backup-plan`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`backupVaultLockCheck`	Das Steuerelement ermittelt, `PASSED` ob der Parameter auf gesetzt ist `true` und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	`true` oder `false`	Kein Standardwert

Dieses Steuerelement bewertet, ob eine Amazon DynamoDB-Tabelle im `ACTIVE` Status durch einen Backup-Plan abgedeckt ist. Die Steuerung schlägt fehl, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, wird die Steuerung nur erfolgreich, wenn die DynamoDB-Tabelle in einem AWS Backup gesperrten Tresor gesichert ist.

AWS Backup ist ein vollständig verwalteter Backup-Service, der Ihnen hilft, die Sicherung von Daten auf allen Ebenen zu zentralisieren und zu automatisieren. AWS-Services Mit AWS Backup können Sie Backup-Pläne erstellen, die Ihre Backup-Anforderungen definieren, z. B. wie oft Ihre Daten gesichert werden sollen und wie lange diese Backups aufbewahrt werden sollen. Wenn Sie DynamoDB-Tabellen in Ihre Backup-Pläne aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer DynamoDB-Tabelle zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[DynamoDB.5] DynamoDB-Tabellen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: `tagged-dynamodb-table` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern

verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DynamoDB-Tabelle finden Sie unter Tagging resources in DynamoDB im Amazon DynamoDB Developer Guide.

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2),, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CM-3, CRI-Profil v2. 2/GV. RM-01.03, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: **`dynamodb-table-deletion-protection-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon DynamoDB-Tabelle der Löschschutz aktiviert ist. Das Steuerelement schlägt fehl, wenn für eine DynamoDB-Tabelle kein Löschschutz aktiviert ist.

Mit der Eigenschaft Löschschutz können Sie eine DynamoDB-Tabelle vor versehentlichem Löschen schützen. Durch die Aktivierung dieser Eigenschaft für Tabellen wird sichergestellt, dass Tabellen nicht versehentlich während der regulären Tabellenverwaltung durch Ihre Administratoren gelöscht werden. Dies trägt dazu bei, Störungen Ihres normalen Geschäftsbetriebs zu vermeiden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine DynamoDB-Tabelle finden Sie unter Verwenden des Löschschutzes im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-17,, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::DAX::Cluster`

AWS Config -Regel: `dax-tls-endpoint-encryption`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DynamoDB Accelerator (DAX) -Cluster während der Übertragung verschlüsselt ist, wobei der Endpunktverschlüsselungstyp auf TLS festgelegt ist. Die Steuerung schlägt fehl, wenn der DAX-Cluster bei der Übertragung nicht verschlüsselt wird.

HTTPS (TLS) kann verwendet werden, um potenzielle Angreifer daran zu hindern, Person-in-the-Middle- oder ähnliche Angriffe zu nutzen, um den Netzwerkverkehr abzuhören oder zu manipulieren. Sie sollten nur verschlüsselte Verbindungen über TLS für den Zugriff auf DAX-Cluster zulassen. Die Verschlüsselung von Daten während der Übertragung kann jedoch die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit aktivierter Verschlüsselung testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Sie können die TLS-Verschlüsselungseinstellung nicht ändern, nachdem Sie einen DAX-Cluster erstellt haben. Um einen vorhandenen DAX-Cluster zu verschlüsseln, erstellen Sie einen neuen

Cluster mit aktivierter Verschlüsselung bei der Übertragung, verlagern Sie den Datenverkehr Ihrer Anwendung darauf und löschen Sie dann den alten Cluster. Weitere Informationen finden Sie unter Verwenden des Löschschutzes im Entwicklerhandbuch zu Amazon DynamoDB.

Security Hub CSPM-Steuerelemente für Amazon EC2

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2). Die Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `ebs-snapshot-public-restorable-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic Block Store-Snapshots so konfiguriert sind, dass sie öffentlich wiederherstellbar sind. Die Steuerung schlägt fehl, wenn Amazon EBS-Snapshots so konfiguriert sind, dass sie von allen wiederhergestellt werden können.

EBS-Snapshots werden verwendet, um die Daten auf Ihren EBS-Volumes zu einem bestimmten Zeitpunkt auf Amazon S3 zu sichern. Sie können die Snapshots verwenden, um frühere Status von EBS-Volumes wiederherzustellen. Es ist selten akzeptabel, einen Snapshot mit der Öffentlichkeit zu teilen. Typischerweise wurde die Entscheidung, eine Momentaufnahme öffentlich zu teilen, irrtümlich

oder ohne vollständiges Verständnis der Auswirkungen getroffen. Diese Überprüfung trägt dazu bei, dass alle diese Freigaben vollständig geplant und beabsichtigt waren.

Abhilfe

Informationen dazu, wie Sie einen öffentlichen EBS-Snapshot privat machen können, finden Sie unter Einen Snapshot teilen im Amazon EC2 EC2-Benutzerhandbuch. Wählen Sie für Aktionen, Berechtigungen ändern die Option Privat aus.

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/55.5, PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/2.1, Benchmark für CIS AWS Foundations v1.2. 0/4.3, Benchmark für CIS AWS Foundations v1.4. 0/5.3, Benchmark v3.0 AWS für CIS Foundations. 0/5.4 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-default-security-group-closed`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Standardsicherheitsgruppe einer VPC eingehenden oder ausgehenden Datenverkehr zulässt. Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe eingehenden oder ausgehenden Datenverkehr zulässt.

Die Regeln für die Standardsicherheitsgruppe erlauben den gesamten ausgehenden und eingehenden Datenverkehr von Netzwerkschnittstellen (und den zugehörigen Instances), die derselben Sicherheitsgruppe zugewiesen sind. Wir empfehlen, die Standardsicherheitsgruppe nicht zu verwenden. Da die Standardsicherheitsgruppe nicht gelöscht werden kann, sollten Sie die Standardeinstellung für Sicherheitsgruppenregeln ändern, um eingehenden und ausgehenden Datenverkehr einzuschränken. Dies verhindert unbeabsichtigten Datenverkehr, wenn die Standardsicherheitsgruppe versehentlich für Ressourcen wie EC2-Instances konfiguriert ist.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie zunächst neue Sicherheitsgruppen mit den geringsten Rechten. Anweisungen finden Sie unter Erstellen einer Sicherheitsgruppe im Amazon VPC-Benutzerhandbuch. Weisen Sie dann die neuen Sicherheitsgruppen Ihren EC2-Instances zu. Anweisungen finden Sie unter Ändern der Sicherheitsgruppe einer Instance im Amazon EC2 EC2-Benutzerhandbuch.

Nachdem Sie Ihren Ressourcen die neuen Sicherheitsgruppen zugewiesen haben, entfernen Sie alle Regeln für eingehenden und ausgehenden Datenverkehr aus den Standardsicherheitsgruppen. Anweisungen finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon VPC-Benutzerhandbuch.

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Volume`

AWS Config -Regel: `encrypted-volumes`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die EBS-Volumes, die sich im angefügten Zustand befinden, verschlüsselt sind. Um diese Prüfung zu bestehen, müssen EBS-Volumes in Betrieb und verschlüsselt sein. Wenn das EBS-Volume nicht angefügt ist, unterliegt es nicht dieser Prüfung.

Um eine zusätzliche Sicherheitsebene Ihrer sensiblen Daten in EBS-Volumes zu gewährleisten, sollten Sie die EBS-Verschlüsselung im Ruhezustand aktivieren. Die Amazon EBS-Verschlüsselung bietet eine einfache Verschlüsselungslösung für Ihre EBS-Ressourcen, ohne dass Sie eine eigene Infrastruktur für die Schlüsselverwaltung erstellen, verwalten und sichern müssen. Bei der Erstellung verschlüsselter Volumes und Snapshots werden KMS-Schlüssel verwendet.

Weitere Informationen zur Amazon EBS-Verschlüsselung finden Sie unter Amazon EBS-Verschlüsselung im Amazon EC2 EC2-Benutzerhandbuch.

Abhilfe

Es gibt keine direkte Möglichkeit, ein vorhandenes unverschlüsseltes Volume oder einen Snapshot zu verschlüsseln. Sie können ein neues Volume oder einen neuen Snapshot nur beim Erstellen verschlüsseln.

Wenn Sie die Verschlüsselung standardmäßig aktiviert haben, verschlüsselt Amazon EBS das resultierende neue Volume oder den Snapshot mit Ihrem Standardschlüssel für die Amazon EBS-Verschlüsselung. Auch wenn Sie die standardmäßige Verschlüsselung nicht aktiviert haben, können Sie die Verschlüsselung beim Erstellen eines einzelnen Volumes oder Snapshots aktivieren.
In beiden Fällen können Sie den Standardschlüssel für die Amazon EBS-Verschlüsselung überschreiben und einen symmetrischen, vom Kunden verwalteten Schlüssel wählen.

Weitere Informationen finden Sie unter Erstellen eines Amazon EBS-Volumes und Kopieren eines Amazon EBS-Snapshots im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/ID. AM-08.01, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Instance`

AWS Config Regel: `ec2-stopped-instance-days-check` (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`AllowedDays`	Anzahl der Tage, an denen sich die EC2-Instance im	Ganzzahl	1 auf 365	30

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	gestoppten Zustand befinden darf, bevor ein fehlgeschlagenes Ergebnis generiert wird.			

Diese Kontrolle prüft, ob eine Amazon EC2 EC2-Instance länger als die zulässige Anzahl von Tagen angehalten wurde. Die Kontrolle schlägt fehl, wenn eine EC2-Instance länger als die maximal zulässige Zeitspanne angehalten wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den maximal zulässigen Zeitraum angeben, verwendet Security Hub CSPM einen Standardwert von 30 Tagen.

Wenn eine EC2-Instance über einen längeren Zeitraum nicht ausgeführt wurde, stellt dies ein Sicherheitsrisiko dar, da die Instance nicht aktiv gewartet (analysiert, gepatcht, aktualisiert) wird. Wenn sie später gestartet wird, kann der Mangel an ordnungsgemäßer Wartung zu unerwarteten Problemen in Ihrer AWS Umgebung führen. Um eine EC2-Instance über einen längeren Zeitraum sicher inaktiv zu halten, starten Sie sie regelmäßig zu Wartungszwecken und beenden Sie sie dann nach der Wartung. Idealerweise sollte dies ein automatisierter Prozess sein.

> **Note**
>
> Dieses Steuerelement bewertet anhand des Zeitstempels `StateTransitionReason` für die Instance die Anzahl der Tage, an denen eine EC2-Instance gestoppt wurde. Wenn das `StateTransitionReason` keinen Zeitstempel enthält (z. B. wenn eine Instance aufgrund eines internen Fehlers gestoppt wurde), verwendet das Steuerelement stattdessen die Startzeit der Instance. Wenn in diesem Fall die Startzeit älter als der maximal zulässige Zeitraum ist, generiert das Steuerelement den Befund FAILED.

Abhilfe

Informationen zum Beenden einer inaktiven EC2-Instance finden Sie unter Terminate an Instance im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.7, Benchmark für CIS AWS Foundations v1.2. 0/2.9, Benchmark für CIS AWS Foundations v1.4. 0/3.9, Benchmark v3.0 für CIS AWS Foundations. 0/3.7, NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20 NIST.800-53.r5 CA-7, NIST.800-171.r2 3.3.1, 3.13.1, NIST.800-171.r2 PCI DSS v3.2. 1/103.3.3, PCI-DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPC`

AWS Config -Regel: `vpc-flow-logs-enabled`

Art des Zeitplans: Periodisch

Parameter:

- `trafficType`: `REJECT` (nicht anpassbar)

Dieses Steuerelement prüft, ob Amazon VPC Flow Logs gefunden und für VPCs aktiviert wurden. Der Datenverkehrstyp ist auf eingestellt. `Reject` Die Steuerung schlägt fehl, wenn VPC Flow Logs für VPCs in Ihrem Konto nicht aktiviert sind.

> **Note**
>
> Dieses Steuerelement überprüft nicht, ob Amazon VPC Flow Logs über Amazon Security Lake für aktiviert sind. AWS-Konto

Mit der Funktion VPC Flow Logs können Sie Informationen über den IP-Adressverkehr zu und von Netzwerkschnittstellen in Ihrer VPC erfassen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die zugehörigen Daten in CloudWatch Logs anzeigen und abrufen. Um die Kosten zu senken, können Sie Ihre Flow-Logs auch an Amazon S3 senden.

Security Hub CSPM empfiehlt, die Flussprotokollierung für Paketablehnungen für VPCs zu aktivieren. Flow-Logs bieten Einblick in den Netzwerkverkehr, der die VPC durchquert, und können anomalen Datenverkehr erkennen oder Einblicke in Sicherheitsworkflows geben.

Standardmäßig enthält der Datensatz Werte für die verschiedenen Komponenten des IP-Adressflusses, einschließlich Quelle, Ziel und Protokoll. Weitere Informationen und Beschreibungen der Protokollfelder finden Sie unter VPC Flow Logs im Amazon VPC-Benutzerhandbuch.

Abhilfe

Informationen zum Erstellen eines VPC-Flow-Protokolls finden Sie unter Erstellen eines Flow-Protokolls im Amazon VPC-Benutzerhandbuch. Nachdem Sie die Amazon VPC-Konsole geöffnet haben, wählen Sie Your VPCs. Wählen Sie für Filter die Option Ablehnen oder Alle.

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/51.1.1, Benchmark für CIS AWS Foundations v1.4. 0/22.2.1, Benchmark v3.0 für CIS AWS Foundations. 0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `ec2-ebs-encryption-by-default`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob die Verschlüsselung auf Kontoebene standardmäßig für Amazon Elastic Block Store (Amazon EBS) -Volumes aktiviert ist. Die Kontrolle schlägt fehl, wenn die Verschlüsselung auf Kontoebene für EBS-Volumes nicht aktiviert ist.

Wenn die Verschlüsselung für Ihr Konto aktiviert ist, werden Amazon EBS-Volumes und Snapshot-Kopien im Ruhezustand verschlüsselt. Dies bietet eine zusätzliche Schutzebene für Ihre Daten. Weitere Informationen finden Sie unter Standardmäßige Verschlüsselung im Amazon-EC2-Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der Standardverschlüsselung für Amazon EBS-Volumes finden Sie unter Standardverschlüsselung im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/5.7, Benchmark v3.0 für CIS AWS Foundations. 0/5.6, NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/2.2.6, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-imdsv2-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre EC2-Instance-Metadatenversion mit Instance Metadata Service Version 2 (IMDSv2) konfiguriert ist. Das Steuerelement ist erfolgreich, wenn `HttpTokens` es für IMDSv2 auf erforderlich gesetzt ist. Das Steuerelement schlägt fehl, wenn auf gesetzt `HttpTokens` ist. `optional`

Sie verwenden Instanz-Metadaten, um die laufende Instanz zu konfigurieren oder zu verwalten. Das IMDS bietet Zugriff auf temporäre, häufig wechselnde Anmeldeinformationen. Mit diesen Anmeldeinformationen entfällt die Notwendigkeit, vertrauliche Anmeldeinformationen manuell oder programmgesteuert fest zu codieren oder vertrauliche Anmeldeinformationen an Instanzen zu verteilen. Das IMDS ist lokal an jede EC2-Instance angehängt. Es läuft auf einer speziellen „Link Local“ -IP-Adresse 169.254.169.254. Auf diese IP-Adresse kann nur mit Software zugegriffen werden, die auf der Instance ausgeführt wird.

Version 2 des IMDS bietet neue Schutzmaßnahmen für die folgenden Arten von Sicherheitslücken. Diese Sicherheitslücken könnten genutzt werden, um zu versuchen, auf das IMDS zuzugreifen.

- Öffnen Sie die Firewalls für Websites und Anwendungen

- Öffnen Sie Reverse-Proxys
- Server-side Sicherheitslücken im Bereich Request Forgery (SSRF)
- Offene Layer-3-Firewalls und Network Address Translation (NAT)

Security Hub CSPM empfiehlt, dass Sie Ihre EC2-Instances mit IMDSv2 konfigurieren.

Abhilfe

Informationen zur Konfiguration von EC2-Instances mit IMDSv2 finden Sie unter Empfohlener Pfad zur Anforderung von IMDSv2 im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI Profile v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.02, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-instance-no-public-ip`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob EC2-Instances eine öffentliche IP-Adresse haben. Die Steuerung schlägt fehl, wenn das `publicIp` Feld im EC2-Instance-Konfigurationselement vorhanden ist. Dieses Steuerelement gilt nur für IPv4-Adressen.

Eine öffentliche IPv4-Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Instance mit einer öffentlichen IP-Adresse starten, ist Ihre EC2-Instance über das Internet erreichbar. Eine private IPv4-Adresse ist eine IP-Adresse, die über das Internet nicht erreichbar ist. Sie können

private IPv4-Adressen für die Kommunikation zwischen EC2-Instances in derselben VPC oder in Ihrem verbundenen privaten Netzwerk verwenden.

IPv6-Adressen sind weltweit einzigartig und daher über das Internet erreichbar. Standardmäßig ist das IPv6-Adressierungsattribut jedoch in allen Subnetzen auf False gesetzt. Weitere Informationen zu IPv6 finden Sie unter IP-Adressierung in Ihrer VPC im Amazon VPC-Benutzerhandbuch.

Wenn Sie einen legitimen Anwendungsfall für die Verwaltung von EC2-Instances mit öffentlichen IP-Adressen haben, können Sie die Ergebnisse dieser Kontrolle unterdrücken. Weitere Informationen zu Frontend-Architekturoptionen finden Sie im AWS Architektur-Blog oder in der AWS Videoserie This Is My Architecture-Serie.

Abhilfe

Verwenden Sie eine nicht standardmäßige VPC, damit Ihrer Instance standardmäßig keine öffentliche IP-Adresse zugewiesen wird.

Wenn Sie eine EC2-Instance in einer Standard-VPC VPC, wird ihr eine öffentliche IP-Adresse zugewiesen. Wenn Sie eine EC2-Instance in einer nicht standardmäßigen VPC starten, bestimmt die Subnetzkonfiguration, ob sie eine öffentliche IP-Adresse erhält. Das Subnetz verfügt über ein Attribut, das bestimmt, ob neue EC2-Instances im Subnetz eine öffentliche IP-Adresse aus dem öffentlichen IPv4-Adresspool erhalten.

Sie können eine automatisch zugewiesene öffentliche IP-Adresse von Ihrer EC2-Instance trennen. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen und externe DNS-Hostnamen im Amazon EC2-Benutzerhandbuch.

[EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, 3.13.1, CRI-Profil v2 NIST.800-171.r2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPC`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

- `serviceNames`: `ec2` (nicht anpassbar)

Dieses Steuerelement prüft, ob für jede VPC ein Service-Endpunkt für Amazon EC2 erstellt wurde. Die Steuerung schlägt fehl, wenn für eine VPC kein VPC-Endpunkt für den Amazon EC2-Service erstellt wurde.

Diese Kontrolle bewertet Ressourcen in einem einzigen Konto. Es kann keine Ressourcen beschreiben, die sich außerhalb des Kontos befinden. Da AWS Config Security Hub CSPM keine kontoübergreifenden Prüfungen durchführt, werden Ihnen `FAILED` Ergebnisse für VPCs angezeigt, die von mehreren Konten gemeinsam genutzt werden. Security Hub CSPM empfiehlt, diese `FAILED` Ergebnisse zu unterdrücken.

Um die Sicherheitslage Ihrer VPC zu verbessern, können Sie Amazon EC2 so konfigurieren, dass es einen VPC-Schnittstellen-Endpunkt verwendet. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Amazon EC2 EC2-API-Operationen zugreifen können. Es schränkt den gesamten Netzwerkverkehr zwischen Ihrer VPC und Amazon EC2 auf das Amazon-Netzwerk ein. Da Endpoints nur in derselben Region unterstützt werden, können Sie keinen Endpunkt zwischen einer VPC und einem Service in einer anderen Region erstellen. Dies verhindert unbeabsichtigte Amazon EC2 EC2-API-Aufrufe in andere Regionen.

Weitere Informationen zum Erstellen von VPC-Endpunkten für Amazon EC2 finden Sie unter Amazon EC2 und Interface-VPC-Endpoints im Amazon EC2 EC2-Benutzerhandbuch.

Abhilfe

Informationen zum Erstellen eines Schnittstellenendpunkts zu Amazon EC2 über die Amazon VPC-Konsole finden Sie unter Erstellen eines VPC-Endpunkts im Handbuch.AWS PrivateLink Wählen Sie für den Servicenamen com.amazonaws aus. ***region***.ec2.

Sie können auch eine Endpunktrichtlinie erstellen und an Ihren VPC-Endpunkt anhängen, um den Zugriff auf die Amazon EC2 EC2-API zu kontrollieren. Anweisungen zum Erstellen einer VPC-Endpunktrichtlinie finden Sie unter Erstellen einer Endpunktrichtlinie im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden

Verwandte Anforderungen: PCI DSS v3.2. 1/2.4, NIST.800-53.r5 CM-8 (1), CRI-Profil v2. 2/ID. AM-08.01, CRI-Profil v2. 2/ID. AM-08.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::EIP`

AWS Config -Regel: `eip-attached`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elastic IP (EIP) -Adressen, die einer VPC zugewiesen sind, an EC2-Instances oder verwendete Elastic Network Interfaces (ENIs) angehängt sind.

Ein fehlgeschlagener Befund deutet darauf hin, dass Sie möglicherweise ungenutzte EC2-EIPs haben.

Auf diese Weise können Sie ein genaues Inventar der EIPs in Ihrer Karteninhaberdatenumgebung (CDE) verwalten.

Abhilfe

Informationen zur Freigabe einer ungenutzten EIP finden Sie unter Eine Elastic IP-Adresse veröffentlichen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/4.1, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1, PCI DSS v3.2. 1/12.2.1, PCI-DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/2.2.2, PCI DSS v4.0. 1/1.3.1, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `restricted-ssh`

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe Zugriffe ab 0.0.0 zulässt. 0/0 oder: :/0 zu Port 22. Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe einen Zugriff ab 0.0.0 zulässt. 0/0oder: :/0 zu Port 22.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Port 22 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie SSH wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugang zu Port 22 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Actions, Edit Inbound Rules. Entfernen Sie die Regel, die den Zugriff auf Port 22 ermöglicht.

[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/42.2, PCI DSS v4.0. 1/1.3.1, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: **`restricted-common-ports`**(Die erstellte Regel ist`restricted-rdp`)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe Zugriffe ab 0.0.0 zulässt. 0/0 oder: :/0 zu Port 3389. Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe einen Zugriff ab 0.0.0 zulässt. 0/0oder: :/0 auf Port 3389.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Port 3389 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie RDP wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugriff auf Port 3389 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon VPC-Benutzerhandbuch. Nachdem Sie in der Amazon VPC-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 3389 ermöglicht.

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Subnet`

AWS Config -Regel: `subnet-auto-assign-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Virtual Private Cloud (Amazon VPC) -Subnetz so konfiguriert ist, dass es automatisch öffentliche IP-Adressen zuweist. Die Steuerung schlägt fehl,

wenn das Subnetz so konfiguriert ist, dass öffentliche IPv4- oder IPv6-Adressen automatisch zugewiesen werden.

Subnetze verfügen über Attribute, die bestimmen, ob Netzwerkschnittstellen automatisch öffentliche IPv4- und IPv6-Adressen erhalten. Für IPv4 ist dieses Attribut auf für Standard-Subnetze und `TRUE` `FALSE` für nicht standardmäßige Subnetze gesetzt (mit Ausnahme von Subnetzen, die nicht dem Standard entsprechen, mit dem EC2 Launch Instance Wizard erstellt wurden, wo es auf gesetzt ist). `TRUE` Für IPv6 ist dieses Attribut standardmäßig auf für alle Subnetze gesetzt. `FALSE` Wenn diese Attribute aktiviert sind, erhalten Instances, die im Subnetz gestartet werden, automatisch die entsprechenden IP-Adressen (IPv4 oder IPv6) auf ihrer primären Netzwerkschnittstelle.

Abhilfe

Informationen zur Konfiguration eines Subnetzes, sodass keine öffentlichen IP-Adressen zugewiesen werden, finden Sie unter Ändern der IP-Adressierungsattribute Ihres Subnetzes im Amazon VPC-Benutzerhandbuch.

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

Verwandte Anforderungen: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0. 1/12.2.7, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config -Regel: `vpc-network-acl-unused-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob es in Ihrer Virtual Private Cloud (VPC) ungenutzte Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) gibt. Die Steuerung schlägt fehl, wenn die Netzwerk-ACL keinem Subnetz zugeordnet ist. Das Steuerelement generiert keine Ergebnisse für eine ungenutzte Standard-Netzwerk-ACL.

Das Steuerelement überprüft die Elementkonfiguration der Ressource `AWS::EC2::NetworkAcl` und bestimmt die Beziehungen der Netzwerk-ACL.

Wenn die einzige Beziehung die VPC der Netzwerk-ACL ist, schlägt die Steuerung fehl.

Wenn andere Beziehungen aufgeführt sind, ist die Kontrolle erfolgreich.

Abhilfe

Anweisungen zum Löschen einer ungenutzten Netzwerk-ACL finden Sie unter Löschen einer Netzwerk-ACL im Amazon VPC-Benutzerhandbuch. Sie können die Standard-Netzwerk-ACL oder eine ACL, die Subnetzen zugeordnet ist, nicht löschen.

[EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-instance-multiple-eni-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine EC2-Instance mehrere Elastic Network Interfaces (ENIs) oder Elastic Fabric Adapters (EFAs) verwendet. Dieses Steuerelement ist erfolgreich, wenn ein einziger Netzwerkadapter verwendet wird. Das Steuerelement enthält eine optionale Parameterliste zur Identifizierung der zulässigen ENIs. Diese Kontrolle schlägt auch fehl, wenn eine EC2-Instance, die zu einem Amazon EKS-Cluster gehört, mehr als eine ENI verwendet. Wenn Ihre EC2-Instances mehrere ENIs als Teil eines Amazon EKS-Clusters benötigen, können Sie diese Kontrollergebnisse unterdrücken.

Mehrere ENIs können zu doppelt vernetzten Instances führen, d. h. zu Instances mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Abhilfe

Informationen zum Trennen einer Netzwerkschnittstelle von einer EC2-Instance finden Sie unter Trennen einer Netzwerkschnittstelle von einer Instance im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-open-only-to-authorized-ports`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`authorizedTcpPorts`	Liste der autorisierten TCP-Ports	IntegerList (mindestens 1 Artikel und maximal 32 Artikel)	1 auf 65535	`[80,443]`
`authorizedUdpPorts`	Liste der autorisierten UDP-Ports	IntegerList (mindestens 1 Artikel und maximal 32 Artikel)	1 auf 65535	Kein Standardwert

Diese Kontrolle prüft, ob eine Amazon EC2-Sicherheitsgruppe uneingeschränkten eingehenden Datenverkehr von nicht autorisierten Ports zulässt. Der Kontrollstatus wird wie folgt bestimmt:

- Wenn Sie den Standardwert für verwendenauthorizedTcpPorts, schlägt die Steuerung fehl, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem anderen Port als den Ports 80 und 443 zulässt.
- Wenn Sie benutzerdefinierte Werte für authorizedTcpPorts oder angeben, schlägt die Steuerung fehlauthorizedUdpPorts, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem nicht aufgelisteten Port zulässt.

Sicherheitsgruppen bieten eine statusabhängige Filterung von eingehendem und ausgehendem Netzwerkverkehr zu. AWS Sicherheitsgruppenregeln sollten dem Prinzip des Zugriffs mit den geringsten Rechten folgen. Uneingeschränkter Zugriff (IP-Adresse mit dem Suffix /0) erhöht die Wahrscheinlichkeit bösartiger Aktivitäten wie Hacking, Denial-of-Service-Angriffe und Datenverlust. Sofern ein Port nicht ausdrücklich zugelassen ist, sollte der Port den uneingeschränkten Zugriff verweigern.

Abhilfe

Informationen zum Ändern einer Sicherheitsgruppe finden Sie unter Arbeiten mit Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2,, (11) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, CRI Profile v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Eingeschränkter Netzwerkzugriff

Schweregrad: Kritisch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: **`restricted-common-ports`**(Die erstellte Regel istvpc-sg-restricted-common-ports)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (nicht anpassbar)

Diese Kontrolle prüft, ob uneingeschränkter eingehender Verkehr für eine Amazon EC2-Sicherheitsgruppe für die angegebenen Ports, die als risikoreich gelten, zugänglich ist. Diese Kontrolle schlägt fehl, wenn eine der Regeln in einer Sicherheitsgruppe eingehenden Datenverkehr ab '0.0.0 zulässt. 0/0' oder ': :/0' zu diesen Ports.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Uneingeschränkter Zugriff (0.0.0. 0/0) erhöht die Wahrscheinlichkeit bösartiger Aktivitäten wie Hacking, Denial-of-Service-Angriffe und Datenverlust. Keine Sicherheitsgruppe sollte uneingeschränkten Zugriff auf die folgenden Ports zulassen:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP 3)
- 135 (PRO STÜCK)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (Go- und Node.js Ruby-Frameworks für die Webentwicklung)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python-Frameworks für die Webentwicklung)
- 5432 (Postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch Armaturenbretter)
- 8080 (Proxy)
- 8088 (älterer HTTP-Port)

- 8888 (alternativer HTTP-Port)
- 9200 oder 9300 () OpenSearch

Abhilfe

Informationen zum Löschen von Regeln aus einer Sicherheitsgruppe finden Sie unter Regeln aus einer Sicherheitsgruppe löschen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.1.13, NIST.800-171.r2 3.1.20, CRI Profile v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPNConnection`

AWS Config -Regel: `vpc-vpn-2-tunnels-up`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Ein VPN-Tunnel ist eine verschlüsselte Verbindung, über die Daten vom Kundennetzwerk zu oder aus AWS einer AWS Site-to-Site VPN-Verbindung übertragen werden können. Jede VPN-Verbindung umfasst zwei VPN-Tunnel, die Sie für eine hohe Verfügbarkeit gleichzeitig verwenden können. Es ist wichtig, sicherzustellen, dass beide VPN-Tunnel für eine VPN-Verbindung verfügbar sind, um eine sichere und hochverfügbare Verbindung zwischen einer AWS VPC und Ihrem Remote-Netzwerk zu bestätigen.

Diese Steuerung überprüft, ob sich beide von VPN bereitgestellten AWS Site-to-Site VPN-Tunnel im UP-Status befinden. Die Steuerung schlägt fehl, wenn sich einer oder beide Tunnel im Status DOWN befinden.

Abhilfe

Informationen zum Ändern der VPN-Tunneloptionen finden Sie unter Ändern der Site-to-Site VPN-Tunneloptionen im AWS Site-to-Site VPN-Benutzerhandbuch.

[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/5.2, Benchmark für CIS AWS Foundations v1.4. 0/5.1, Benchmark v3.0 AWS für CIS Foundations. 0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2,, (21) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, PCI DSS v4.0. 1/1.3.1, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config -Regel: `nacl-no-unrestricted-ssh-rdp`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Netzwerkzugriffskontrollliste (Network Access Control List, Netzwerk-ACL) uneingeschränkten Zugriff auf die Standard-TCP-Ports für SSH/RDP eingehenden Datenverkehr ermöglicht. Die Steuerung schlägt fehl, wenn der eingehende Netzwerk-ACL-Eintrag einen Quell-CIDR-Block von '0.0.0 zulässt. 0/0' oder ': :/0' für die TCP-Ports 22 oder 3389. Das Steuerelement generiert keine Ergebnisse für eine Standard-Netzwerk-ACL.

Der Zugriff auf Remoteserveradministrationsports, wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.

Abhilfe

Informationen zum Bearbeiten von Netzwerk-ACL-Traffic-Regeln finden Sie unter Arbeiten mit Netzwerk-ACLs im Amazon VPC-Benutzerhandbuch.

[EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config -Regel: `ec2-security-group-attached-to-eni-periodic`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Sicherheitsgruppen an Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder an eine elastic network interface angehängt sind. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keiner Amazon EC2 EC2-Instance oder einer elastic network interface zugeordnet ist.

> **Important**
>
> Am 20. September 2023 hat Security Hub CSPM diese Kontrolle aus den Standards AWS Foundation Security Best Practices und NIST SP 800-53 Revision 5 entfernt. Diese Kontrolle ist weiterhin Teil des Service-Managed-Standards. AWS Control Tower Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2-Instances oder eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2-Steuerelemente wie EC2.2,, und verwenden EC2.13 EC2.14 EC2.18, um Ihre Sicherheitsgruppen zu überwachen EC2.19.

Abhilfe

Informationen zum Erstellen, Zuweisen und Löschen von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::TransitGateway`

AWS Config -Regel: `ec2-transit-gateway-auto-vpc-attach-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob EC2-Transit-Gateways gemeinsam genutzte VPC-Anhänge automatisch akzeptieren. Diese Steuerung schlägt bei einem Transit-Gateway fehl, das automatisch gemeinsame VPC-Anhangsanforderungen akzeptiert.

Durch die Aktivierung wird ein Transit-Gateway so `AutoAcceptSharedAttachments` konfiguriert, dass es automatisch alle kontoübergreifenden VPC-Anhangsanforderungen akzeptiert, ohne die Anfrage oder das Konto, von dem der Anhang stammt, zu überprüfen. Um den bewährten Methoden der Autorisierung und Authentifizierung zu folgen, empfehlen wir, diese Funktion zu deaktivieren, um sicherzustellen, dass nur autorisierte VPC-Anhangsanfragen akzeptiert werden.

Abhilfe

Informationen zum Ändern eines Transit-Gateways finden Sie unter Modifizieren eines Transit-Gateways im Amazon VPC Developer Guide.

[EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

Verwandte Anforderungen: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI Profile v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-paravirtual-instance-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Virtualisierungstyp einer EC2-Instance paravirtuell ist. Die Steuerung schlägt fehl, wenn der Wert `virtualizationType` der EC2-Instance auf gesetzt ist. `paravirtual`

Linux Amazon Machine Images (AMIs) verwenden eine von zwei Arten der Virtualisierung: paravirtuelle (PV) oder virtuelle Hardware-Maschine (HVM). Die Hauptunterschiede zwischen PV- und HVM-AMIs sind die Art und Weise, wie sie gestartet werden und ob sie spezielle Hardwareerweiterungen (CPU, Netzwerk und Speicher) zur Verbesserung der Leistung nutzen können.

Früher verfügten PV-Gäste in vielen Fällen über eine bessere Leistung als HVM-Gäste, aber aufgrund von Verbesserungen der HVM-Virtualisierung und der Verfügbarkeit von PV-Treibern für HVM-AMIs ist dies nicht mehr der Fall. Weitere Informationen finden Sie unter Linux-AMI-Virtualisierungstypen im Amazon EC2 EC2-Benutzerhandbuch.

Abhilfe

Informationen zum Aktualisieren einer EC2-Instance auf einen neuen Instance-Typ finden Sie unter Ändern des Instance-Typs im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::LaunchTemplate`

AWS Config -Regel: `ec2-launch-template-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon EC2 EC2-Startvorlagen so konfiguriert sind, dass Netzwerkschnittstellen beim Start öffentliche IP-Adressen zugewiesen werden. Die Steuerung schlägt fehl, wenn eine EC2-Startvorlage so konfiguriert ist, dass Netzwerkschnittstellen eine öffentliche IP-Adresse zugewiesen wird.

Eine öffentliche IP-Adresse ist eine, die über das Internet erreichbar ist. Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die mit diesen Netzwerkschnittstellen verknüpften Ressourcen möglicherweise vom Internet aus erreichbar. EC2-Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Workloads ermöglichen kann.

Abhilfe

Informationen zum Aktualisieren einer EC2-Startvorlage finden Sie unter Ändern der Standardeinstellungen für die Netzwerkschnittstelle im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden

Kategorie: Wiederherstellen > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Volume`

AWS Config Regel: **`ebs-resources-protected-by-backup-plan`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`backupVaultLockCheck`	Das Steuerelement ermittelt, `PASSED` ob der Parameter auf gesetzt ist `true` und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	`true` oder `false`	Kein Standardwert

Diese Kontrolle bewertet, ob ein Amazon EBS-Volume im `in-use` Status durch einen Backup-Plan abgedeckt ist. Die Kontrolle schlägt fehl, wenn ein EBS-Volume nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, ist die Steuerung nur erfolgreich, wenn das EBS-Volume in einem AWS Backup gesperrten Tresor gesichert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Wenn Sie Amazon EBS-Volumes in einen Backup-Plan aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen eines Amazon EBS-Volumes zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[EC2.33] EC2 Transit Gateway-Anhänge sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayAttachment`

AWS Config Regel: `tagged-ec2-transitgatewayattachment` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon EC2-Transit-Gateway-Anhang Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn der Transit-Gateway-Anhang keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Transit-Gateway-Anhang mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Transit Gateway-Anhang finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayRouteTable`

AWS Config Regel: `tagged-ec2-transitgatewayroutetable` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2-Transit-Gateway-Routentabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Transit-Gateway-Routentabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Transit-Gateway-Routentabelle mit keinem Schlüssel

gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Transit-Gateway-Routentabelle finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkInterface`

AWS Config Regel: `tagged-ec2-networkinterface` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Netzwerkschnittstelle Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Netzwerkschnittstelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerkschnittstelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Netzwerkschnittstelle finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::CustomerGateway`

AWS Config Regel: `tagged-ec2-customergateway` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Kunden-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das Kunden-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Kunden-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Kunden-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::EIP`

AWS Config Regel: `tagged-ec2-eip` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Elastic IP-Adresse Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Elastic IP-Adresse keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Elastic IP-Adresse mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Elastic IP-Adresse finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.38] EC2-Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Instance`

AWS Config Regel: `tagged-ec2-instance` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Instanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Instance finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.39] EC2-Internet-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::InternetGateway`

AWS Config Regel: `tagged-ec2-internetgateway` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Internet-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Internet-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Internet-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Internet-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.40] EC2-NAT-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NatGateway`

AWS Config Regel: `tagged-ec2-natgateway` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Gateway zur Netzwerkadressübersetzung (NAT) Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das NAT-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das NAT-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-NAT-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.41] EC2-Netzwerk-ACLs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config Regel: `tagged-ec2-networkacl` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Netzwerkzugriffskontrollliste (Network ACL) Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn die Netzwerk-ACL keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerk-ACL mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Netzwerk-ACL finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::RouteTable`

AWS Config Regel: `tagged-ec2-routetable` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Routentabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Routing-Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Routing-Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Routing-Tabelle finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.43] EC2-Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: `tagged-ec2-securitygroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Sicherheitsgruppe finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.44] EC2-Subnetze sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Subnet`

AWS Config Regel: `tagged-ec2-subnet` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2-Subnetz Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn das Subnetz keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Subnetz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Subnetz finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.45] EC2-Volumes sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Volume`

AWS Config Regel: `tagged-ec2-volume` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Volume Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Volume keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Volume mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Volume finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.46] Amazon VPCs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPC`

AWS Config Regel: `tagged-ec2-vpc` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Virtual Private Cloud (Amazon VPC) Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Amazon VPC keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Amazon VPC mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer VPC finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.47] Amazon VPC Endpoint Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPCEndpointService`

AWS Config Regel: `tagged-ec2-vpcendpointservice` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon VPC-Endpunktservice über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Endpunkt-Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Endpunktdienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Endpunktservice finden Sie unter Tags verwalten im Abschnitt Konfiguration eines Endpunktdienstes des AWS PrivateLink Handbuchs.

[EC2.48] Amazon VPC-Flow-Logs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::FlowLog`

AWS Config Regel: `tagged-ec2-flowlog` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon VPC-Flow-Log Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Flow-Protokoll keine Tag-Schlüssel enthält oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Flow-Protokoll mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Flow-Protokoll finden Sie unter Taggen eines Flow-Protokolls im Amazon VPC-Benutzerhandbuch.

[EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPCPeeringConnection`

AWS Config Regel: `tagged-ec2-vpcpeeringconnection` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon VPC-Peering-Verbindung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Peering-Verbindung keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Peering-Verbindung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon VPC-Peering-Verbindung finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.50] EC2-VPN-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPNGateway`

AWS Config Regel: `tagged-ec2-vpngateway` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-VPN-Gateway über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das VPN-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das VPN-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-VPN-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (7), NIST.800-53.r5

AU-9 (9), NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 CA-7,, NIST.800-53.r5 SI-3 (20), (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-171.r2 3.1.12, NIST.800-53.r5 SI-7 3.1.20, PCI DSS NIST.800-171.r2 v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::ClientVpnEndpoint`

AWS Config Regel: **`ec2-client-vpn-connection-log-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen AWS Client VPN Endpunkt die Client-Verbindungsprotokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für den Endpunkt die Client-Verbindungsprotokollierung nicht aktiviert ist.

Client-VPN-Endpunkte ermöglichen Remote-Clients die sichere Verbindung zu Ressourcen in einer Virtual Private Cloud (VPC) in. AWS Verbindungsprotokolle ermöglichen es Ihnen, Benutzeraktivitäten auf dem VPN-Endpunkt zu verfolgen und bieten Transparenz. Wenn Sie die Verbindungsprotokollierung aktivieren, können Sie den Namen eines Protokolldatenstroms in der Protokollgruppe angeben. Wenn Sie keinen Protokollstream angeben, erstellt der Client-VPN-Dienst einen für Sie.

Abhilfe

Informationen zum Aktivieren der Verbindungsprotokollierung finden Sie unter Aktivieren der Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt im AWS Client VPN Administratorhandbuch.

[EC2.52] EC2-Transit-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGateway`

AWS Config Regel: `tagged-ec2-transitgateway` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon EC2-Transit-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das Transit-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Transit-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Transit-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/5.3, Benchmark v3.0 AWS für CIS Foundations. 0/5.2, PCI DSS v4.0. 1/1.3.1, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-port-restriction-check`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`ipType`	Die IP-Version	Zeichenfolge	Nicht anpassbar	`IPv4`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`restrictPorts`	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	`22,3389`

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe Zugriffe ab 0.0.0 zulässt. 0/0 zu den Ports für die Remote-Serververwaltung (Ports 22 und 3389). Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe einen Zugriff ab Version 0.0.0 zulässt. 0/0 zu Port 22 oder 3389.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2-Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Actions, Edit Inbound Rules. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/5.4, Benchmark v3.0 für CIS AWS Foundations. 0/5.3, PCI DSS v4.0. 1/13.3.1, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-port-restriction-check`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`ipType`	Die IP-Version	Zeichenfolge	Nicht anpassbar	`IPv6`
`restrictPorts`	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	`22,3389`

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe den Zugriff von: :/0 zu den Remote-Serververwaltungsports (Ports 22 und 3389) zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugang von: :/0 zu Port 22 oder 3389 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2-Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Actions, Edit Inbound Rules. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

[EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`serviceNames`	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	Zeichenfolge	Nicht anpassbar	`ecr.api`
`vpcIds`	Optional	Comma-separated Liste der Amazon VPC-IDs für VPC-	StringList	Mit einer oder mehreren VPC-IDs anpassen	Kein Standardwert

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
		Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im `serviceName` Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.			

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für die Amazon ECR-API verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für die ECR-API hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die von ihrer VPC oder ihren lokalen Standorten PrivateLink aus betrieben werden, ohne öffentliche IPs zu verwenden und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im AWS PrivateLink Handbuch.

[EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`serviceNames`	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	Zeichenfolge	Nicht anpassbar	`ecr.dkr`
`vpcIds`	Optional	Comma-separated Liste der	StringList	Mit einer oder mehreren	Kein Standardwert

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
		Amazon VPC-IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im `serviceName` Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.		VPC-IDs anpassen	

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für Docker Registry verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Docker Registry hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die von ihrer VPC oder ihren lokalen

Standorten PrivateLink aus betrieben werden, ohne öffentliche IPs zu verwenden und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im AWS PrivateLink Handbuch.

[EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`serviceNames`	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	Zeichenfolge	Nicht anpassbar	`ssm`

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`vpcIds`	Optional	Comma-separated Liste der Amazon VPC-IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im `serviceName` Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.	StringList	Mit einer oder mehreren VPC-IDs anpassen	Kein Standardwert

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt verfügt. AWS Systems Manager Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die von ihrer VPC oder ihren lokalen Standorten PrivateLink aus betrieben werden, ohne öffentliche IPs zu verwenden und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im AWS PrivateLink Handbuch.

[EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`serviceNames`	Erforderlich	Der Name des Dienstes, den das	Zeichenfolge	Nicht anpassbar	`ssm-contacts`

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
		Steuerelement auswertet			
`vpcIds`	Optional	Comma-separated Liste der Amazon VPC-IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im `serviceName` Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.	StringList	Mit einer oder mehreren VPC-IDs anpassen	Kein Standardwert

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für AWS Systems Manager Incident Manager-Kontakte verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager Incident Manager-Kontakte hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die von ihrer VPC oder ihren lokalen Standorten PrivateLink aus betrieben werden, ohne öffentliche IPs zu verwenden und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im AWS PrivateLink Handbuch.

[EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config -Regel: vpc-endpoint-enabled

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`serviceNames`	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	Zeichenfolge	Nicht anpassbar	`ssm-incidents`
`vpcIds`	Optional	Comma-separated Liste der Amazon VPC-IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im `serviceName` Parameter angegebenen Dienste keinen dieser VPC-	StringList	Mit einer oder mehreren VPC-IDs anpassen	Kein Standardwert

Parameter	Erforderlich	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
		Endpunkte haben.			

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für AWS Systems Manager Incident Manager verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager Incident Manager hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die von ihrer VPC oder ihren lokalen Standorten PrivateLink aus betrieben werden, ohne öffentliche IPs zu verwenden und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im AWS PrivateLink Handbuch.

[EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

Verwandte Anforderungen: PCI DSS v4.0. 1/22.2.6, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::LaunchTemplate`

AWS Config -Regel: ec2-launch-template-imdsv2-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Startvorlage mit Instance Metadata Service Version 2 (IMDSv2) konfiguriert ist. Die Steuerung schlägt fehl, wenn sie auf gesetzt `HttpTokens` ist. `optional`

Das Ausführen von Ressourcen auf unterstützten Softwareversionen gewährleistet optimale Leistung, Sicherheit und Zugriff auf die neuesten Funktionen. Regelmäßige Updates schützen vor Sicherheitslücken und sorgen so für ein stabiles und effizientes Benutzererlebnis.

Abhilfe

Informationen zur Anforderung von IMDSv2 für eine EC2-Startvorlage finden Sie unter Configure the Instance Metadata Service options im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0. 0/51.3, PCI DSS v4.0. 1/10.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPNConnection`

AWS Config -Regel: ec2-vpn-connection-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei einer AWS Site-to-Site VPN-Verbindung Amazon CloudWatch Logs für beide Tunnel aktiviert ist. Die Kontrolle schlägt fehl, wenn bei einer Site-to-Site VPN-Verbindung CloudWatch Logs nicht für beide Tunnel aktiviert sind.

AWS Site-to-Site VPN-Protokolle bieten Ihnen einen tieferen Einblick in Ihre Site-to-Site VPN-Bereitstellungen. Mit dieser Funktion haben Sie Zugriff auf Site-to-Site VPN-Verbindungsprotokolle, die Details zur Einrichtung eines IPSec-Tunnels (IPSec), zu IKE-Verhandlungen (Internet Key Exchange) und zu DPD-Protokollnachrichten (Dead Peer Detection) enthalten. Site-to-Site VPN-Protokolle können in Logs veröffentlicht werden. CloudWatch Diese Funktion bietet Kunden eine einzige konsistente Möglichkeit, auf detaillierte Protokolle für all ihre Site-to-Site VPN-Verbindungen zuzugreifen und diese zu analysieren.

Abhilfe

Informationen zur Aktivierung der Tunnelprotokollierung für eine EC2-VPN-Verbindung finden Sie unter AWS Site-to-Site VPN-Protokolle im AWS Site-to-Site VPN-Benutzerhandbuch.

[EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config Regel: `ec2-vpc-bpa-internet-gateway-blocked` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`vpcBpaInternetGatewayBlockMode`	Zeichenkettenwert des VPC BPA-Optionsmodus.	Enum	`block-bidirectional` , `block-ingress`	Kein Standardwert

Dieses Steuerelement prüft, ob die Amazon EC2 VPC Block Public Access (BPA) -Einstellungen so konfiguriert sind, dass der Internet-Gateway-Verkehr für alle Amazon VPCs in der blockiert wird. AWS-Konto Die Steuerung schlägt fehl, wenn die VPC BPA-Einstellungen nicht so konfiguriert sind, dass sie den Internet-Gateway-Verkehr blockieren. Damit die Kontrolle erfolgreich ist, `InternetGatewayBlockMode` muss der VPC BPA auf oder gesetzt sein`block-bidirectional`. `block-ingress` Wenn der Parameter angegeben

`vpcBpaInternetGatewayBlockMode` wird, wird die Steuerung nur erfolgreich ausgeführt, wenn der VPC BPA-Wert für `InternetGatewayBlockMode` mit dem Parameter übereinstimmt.

Wenn Sie die VPC-BPA-Einstellungen für Ihr Konto in einem konfigurieren, AWS-Region können Sie verhindern, dass Ressourcen in VPCs und Subnetzen, die Sie in dieser Region besitzen, über Internet-Gateways und Internet-Gateways nur für ausgehenden Verkehr über das Internet erreichen oder von dort aus erreicht werden. Wenn Sie bestimmte VPCs und Subnetze benötigen, um auf das Internet zuzugreifen oder über das Internet erreichbar zu sein, können Sie diese ausschließen, indem Sie VPC-BPA-Ausschlüsse konfigurieren. Anweisungen zum Erstellen und Löschen von Ausschlüssen finden Sie unter Ausnahmen erstellen und löschen im Amazon VPC-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von bidirektionalem BPA auf Kontoebene finden Sie unter Bidirektionalen BPA-Modus für Ihr Konto aktivieren im Amazon VPC-Benutzerhandbuch. Informationen zum Aktivieren von BPA nur für eingehenden Datenverkehr finden Sie unter Ändern des VPC-BPA-Modus auf Nur eingehenden Datenverkehr. Informationen zur Aktivierung von VPC BPA auf Organisationsebene finden Sie unter Aktivieren von VPC BPA auf Organisationsebene.

[EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::SpotFleet`

AWS Config -Regel: ec2-spot-fleet-request-ct-encryption-at-rest

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon EC2 Spot Fleet-Anfrage, die Startparameter spezifiziert, so konfiguriert ist, dass die Verschlüsselung für alle Amazon Elastic Block Store (Amazon EBS) -Volumes (Amazon EBS) aktiviert wird, die an EC2-Instances angehängt sind. Die Kontrolle schlägt fehl, wenn die Spot-Fleet-Anfrage Startparameter spezifiziert und die Verschlüsselung für ein oder mehrere in der Anfrage angegebene EBS-Volumes nicht aktiviert.

Für eine zusätzliche Sicherheitsebene sollten Sie die Verschlüsselung für Amazon EBS-Volumes aktivieren. Verschlüsselungsvorgänge finden dann auf den Servern statt, die Amazon EC2 EC2-Instances hosten, wodurch die Sicherheit sowohl der ruhenden Daten als auch der Daten während der Übertragung zwischen einer Instance und dem angeschlossenen EBS-Speicher gewährleistet wird. Die Amazon EBS-Verschlüsselung ist eine einfache Verschlüsselungslösung für EBS-Ressourcen, die mit Ihren EC2-Instances verknüpft sind. Mit der EBS-Verschlüsselung müssen Sie keine eigene Schlüsselverwaltungsinfrastruktur aufbauen, verwalten und sichern. Die EBS-Verschlüsselung wird AWS KMS keys bei der Erstellung verschlüsselter Volumes verwendet.

> **Hinweise**
>
> Dieses Steuerelement generiert keine Ergebnisse für Amazon EC2 Spot Fleet-Anfragen, die Startvorlagen verwenden. Es generiert auch keine Ergebnisse für Spot-Flotte-Anfragen, die nicht explizit einen Wert für den `encrypted` Parameter angeben.

Abhilfe

Es gibt keine direkte Möglichkeit, ein vorhandenes, unverschlüsseltes Amazon EBS-Volume zu verschlüsseln. Sie können ein neues Volume nur verschlüsseln, wenn Sie es erstellen.

Wenn Sie jedoch die Verschlüsselung standardmäßig aktivieren, verschlüsselt Amazon EBS neue Volumes mithilfe Ihres Standardschlüssels für die EBS-Verschlüsselung. Wenn Sie die Verschlüsselung nicht standardmäßig aktivieren, können Sie die Verschlüsselung aktivieren, wenn Sie ein einzelnes Volume erstellen. In beiden Fällen können Sie den Standardschlüssel für die EBS-Verschlüsselung außer Kraft setzen und einen vom Kunden verwalteten AWS KMS key Schlüssel auswählen. Weitere Informationen zur EBS-Verschlüsselung finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

Informationen zum Erstellen einer Amazon EC2 Spot Fleet-Anfrage finden Sie unter Create a Spot Fleet im Amazon Elastic Compute Cloud-Benutzerhandbuch.

[EC2.174] EC2-DHCP-Optionssätze sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::DHCPOptions`

AWS Config -Regel: ec2-dhcp-options-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-DHCP-Optionssatz die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn der Optionssatz keine Tag-Schlüssel oder nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Optionssatz keine Tag-Schlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2 DHCP-Optionssatz finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::LaunchTemplate`

AWS Config -Regel: ec2-launch-template-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Startvorlage die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Startvorlage keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Startvorlage keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon EC2 EC2-Startvorlage finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::PrefixList`

AWS Config -Regel: ec2-prefix-list-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2-Präfixliste die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Präfixliste keine Tag-Schlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Präfixliste keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon EC2-Präfixliste finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorSession`

AWS Config -Regel: ec2-traffic-mirror-session-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2-Traffic-Mirror-Sitzung die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Sitzung keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Sitzung keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon EC2-Traffic-Mirror-Sitzung finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorFilter`

AWS Config -Regel: ec2-traffic-mirror-filter-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2-Traffic-Mirror-Filter über die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Filter keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Filter keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2-Traffic-Mirror-Filter finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorTarget`

AWS Config -Regel: ec2-traffic-mirror-target-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2-Traffic-Mirror-Ziel über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Die Steuerung schlägt fehl, wenn das Ziel keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Ziel keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2-Traffic-Mirror-Ziel finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination

Verwandte Anforderungen: CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::NetworkInterface`

AWS Config -Regel: ec2-enis-source-destination-check-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die source/destination Prüfung für ein Amazon EC2 elastic network interface (ENI) aktiviert ist, das von Benutzern verwaltet wird. Die Steuerung schlägt fehl, wenn die source/destination Prüfung für das benutzerverwaltete ENI deaktiviert ist. Dieses Steuerelement überprüft nur die folgenden Typen von ENIs:`aws_codestar_connections_managed`,,`branch`, `efa` `interfacelambda`, und. `quicksight`

Source/destination Die Suche nach Amazon EC2 EC2-Instances und angehängten ENIs sollte für alle EC2-Instances aktiviert und konsistent konfiguriert sein. Jede ENI hat ihre eigene Einstellung für Prüfungen. source/destination Wenn die source/destination Prüfung aktiviert ist, erzwingt Amazon EC2 die source/destination Adressvalidierung, wodurch sichergestellt wird, dass eine Instance entweder die Quelle oder das Ziel des empfangenen Datenverkehrs ist. Dies bietet eine zusätzliche Netzwerksicherheitsebene, indem verhindert wird, dass Ressourcen unbeabsichtigten Datenverkehr verarbeiten, und das Spoofing von IP-Adressen verhindert wird.

> **Note**
>
> Wenn Sie eine EC2-Instance als NAT-Instance verwenden und die source/destination Überprüfung auf ihre ENI deaktiviert haben, können Sie stattdessen ein NAT-Gateway verwenden.

Abhilfe

Informationen zur Aktivierung von source/destination Prüfungen für eine Amazon EC2 EC2-ENI finden Sie unter Ändern von Netzwerkschnittstellenattributen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::LaunchTemplate`

AWS Config -Regel: ec2-launch-templates-ebs-volume-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon EC2 EC2-Startvorlage die Verschlüsselung für alle angehängten EBS-Volumes aktiviert. Die Kontrolle schlägt fehl, wenn der Verschlüsselungsparameter `False` für alle EBS-Volumes, die in der EC2-Startvorlage angegeben sind, auf gesetzt ist.

Die Amazon EBS-Verschlüsselung ist eine einfache Verschlüsselungslösung für EBS-Ressourcen, die Amazon EC2 EC2-Instances zugeordnet sind. Mit der EBS-Verschlüsselung müssen Sie keine eigene Schlüsselverwaltungsinfrastruktur aufbauen, warten und sichern. Die EBS-Verschlüsselung wird AWS KMS keys bei der Erstellung verschlüsselter Volumes und Snapshots verwendet. Verschlüsselungsvorgänge finden auf den Servern statt, die EC2-Instances hosten. Dadurch wird die Sicherheit von Daten im Ruhezustand und bei der Übertragung zwischen einer EC2-Instance und dem angeschlossenen EBS-Speicher gewährleistet. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EBS-Benutzerhandbuch.

Sie können die EBS-Verschlüsselung beim manuellen Start einzelner EC2-Instances aktivieren. Die Verwendung von EC2-Startvorlagen und die Konfiguration der Verschlüsselungseinstellungen in diesen Vorlagen bieten jedoch mehrere Vorteile. Sie können die Verschlüsselung als Standard erzwingen und die Verwendung einheitlicher Verschlüsselungseinstellungen sicherstellen. Sie können auch das Risiko von Fehlern und Sicherheitslücken verringern, die beim manuellen Starten von Instances auftreten können.

> **Note**
>
> Wenn dieses Steuerelement eine EC2-Startvorlage überprüft, werden nur EBS-Verschlüsselungseinstellungen ausgewertet, die in der Vorlage explizit angegeben sind. Die Bewertung umfasst keine Verschlüsselungseinstellungen, die von EBS-Verschlüsselungseinstellungen auf Kontoebene, AMI-Blockgerätezuordnungen oder Quell-Snapshot-Verschlüsselungsstatus übernommen wurden.

Abhilfe

Nachdem Sie eine Amazon EC2 EC2-Startvorlage erstellt haben, können Sie sie nicht mehr ändern. Sie können jedoch eine neue Version einer Startvorlage erstellen und die Verschlüsselungseinstellungen in dieser neuen Version der Vorlage ändern. Sie können die neue Version auch als Standardversion der Startvorlage angeben. Wenn Sie dann eine EC2-Instance von einer Startvorlage aus starten und keine Vorlagenversion angeben, verwendet EC2 beim Starten der Instance die Einstellungen der Standardversion. Weitere Informationen finden Sie unter Ändern einer Startvorlage im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SnapshotBlockPublicAccess`

AWS Config -Regel: ebs-snapshot-block-public-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Sperrung des öffentlichen Zugriffs auf Kontoebene aktiviert ist, um zu verhindern, dass Amazon EBS-Snapshots an alle weitergegeben werden. Die Steuerung schlägt fehl, wenn Block Public Access nicht aktiviert ist, um die gemeinsame Nutzung von Amazon EBS-Snapshots für alle zu blockieren.

Um zu verhindern, dass Ihre Amazon EBS-Snapshots öffentlich geteilt werden, können Sie den öffentlichen Zugriff für Snapshots sperren aktivieren. Sobald die Sperrung des öffentlichen Zugriffs für Snapshots in einer Region aktiviert ist, wird jeder Versuch, Snapshots in dieser Region öffentlich zu teilen, automatisch blockiert. Dies trägt dazu bei, die Sicherheit der Snapshots zu verbessern und die Snapshot-Daten vor unbefugtem oder unbeabsichtigtem Zugriff zu schützen.

Abhilfe

Informationen zum Aktivieren des blockierten öffentlichen Zugriffs für Snapshots finden Sie unter Konfiguration des blockierten öffentlichen Zugriffs für Amazon EBS-Snapshots im Amazon

EBS-Benutzerhandbuch. Wählen Sie unter Öffentlichen Zugriff blockieren die Option Gesamten öffentlichen Zugriff blockieren aus.

[EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPNConnection`

AWS Config -Regel: ec2-vpn-connection-ike-version-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS Site-to-Site VPN-Verbindung für die Verwendung des IKEv2-Protokolls konfiguriert ist. Die Steuerung schlägt fehl, wenn eine Site-to-Site VPN-Verbindung das IKEv1-Protokoll zulässt oder nicht in allen VPN-Tunneln explizit auf IKEv2 beschränkt ist.

IKEv2 bietet im Vergleich zum alten IKEv1-Protokoll stärkere kryptografische Algorithmen und verbesserte Sicherheitsfunktionen, einschließlich integriertem Schutz vor Denial-of-Service-Angriffen und erweiterten Authentifizierungsmechanismen. IKEv1 weist bekannte Sicherheitslücken und Schwächen in seinem Schlüsselaustauschprozess auf, die von Angreifern ausgenutzt werden können, um die Sicherheit des VPN-Tunnels zu gefährden. Durch die Durchsetzung von IKEv2-only Verbindungen reduzieren Sie Ihre Angriffsfläche und stellen sicher, dass bei der VPN-Kommunikation moderne, branchenübliche Verschlüsselungsprotokolle verwendet werden, die Daten während der Übertragung besser schützen.

Abhilfe

Informationen zum Aktualisieren der IKE-Version für einen VPN-Tunnel auf einer EC2-VPN-Verbindung finden Sie unter Ändern der AWS Site-to-Site VPN-Tunneloptionen im AWS Site-to-Site VPN-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Auto Scaling

Diese Security Hub CSPM-Steuerungen bewerten den Service und die Ressourcen von Amazon EC2 Auto Scaling.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

Verwandte Anforderungen: PCI DSS v3.2. 1/2.2, NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2 (2) NIST.800-53.r5 SI-2, CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-group-elb-healthcheck-required`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe, die einem Load Balancer zugeordnet ist, Elastic Load Balancing (ELB) -Zustandsprüfungen verwendet. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine ELB-Zustandsprüfungen verwendet.

ELB-Zustandsprüfungen stellen sicher, dass eine Auto Scaling Scaling-Gruppe den Zustand einer Instance anhand zusätzlicher Tests ermitteln kann, die vom Load Balancer bereitgestellt werden. Die Verwendung von Elastic Load Balancing Health Checks trägt auch dazu bei, die Verfügbarkeit von Anwendungen zu unterstützen, die EC2 Auto Scaling Scaling-Gruppen verwenden.

Abhilfe

Informationen zum Hinzufügen von Elastic Load Balancing Balancing-Zustandsprüfungen finden Sie unter Elastic Load Balancing Balancing-Zustandsprüfungen hinzufügen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-multiple-az`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mindestens die angegebene Anzahl von Availability Zones (AZs) umfasst. Die Steuerung schlägt fehl, wenn eine Auto Scaling Scaling-Gruppe nicht mindestens die angegebene Anzahl von AZs umfasst. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub CSPM einen Standardwert von zwei AZs.

Eine Auto Scaling Scaling-Gruppe, die sich nicht über mehrere AZs erstreckt, kann keine Instances in einer anderen AZ starten, um dies zu kompensieren, wenn die konfigurierte einzelne AZ nicht mehr verfügbar ist. In einigen Anwendungsfällen kann jedoch eine Auto Scaling Scaling-Gruppe mit einer einzigen Availability Zone bevorzugt werden, z. B. bei Batch-Jobs oder wenn die Inter-AZ-Übertragungskosten auf ein Minimum beschränkt werden müssen. In solchen Fällen können Sie diese Steuerung deaktivieren oder ihre Ergebnisse unterdrücken.

Abhilfe

Informationen zum Hinzufügen von AZs zu einer vorhandenen Auto Scaling Scaling-Gruppe finden Sie unter Availability Zones hinzufügen und entfernen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6 NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.6, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launchconfig-requires-imdsv2`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob IMDSv2 auf allen Instances aktiviert ist, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden. Die Steuerung schlägt fehl, wenn die Version des Instance Metadata Service (IMDS) nicht in der Startkonfiguration enthalten ist oder als konfiguriert ist`token optional`, was eine Einstellung ist, die entweder IMDSv1 oder IMDSv2 zulässt.

IMDS stellt Daten über Ihre Instance bereit, die Sie verwenden können, um die laufende Instance zu konfigurieren oder zu verwalten.

Version 2 des IMDS fügt neue Schutzmaßnahmen hinzu, die in IMDSv1 nicht verfügbar waren, um Ihre EC2-Instances weiter zu schützen.

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration für eine Auto Scaling Scaling-Gruppe zu ändern, verwenden Sie eine bestehende Startkonfiguration als Grundlage für eine neue Startkonfiguration mit aktiviertem IMDSv2. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances im Amazon EC2 EC2-Benutzerhandbuch.

[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit von mehr als 1 haben

> **Important**
>
> Security Hub CSPM hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub CSPM-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launch-config-hop-limit`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft die Anzahl der Netzwerk-Hops, die ein Metadaten-Token zurücklegen kann. Die Steuerung schlägt fehl, wenn das Limit für Metadaten-Antwort-Hops größer als ist1.

Der Instance Metadata Service (IMDS) stellt Metadateninformationen zu einer Amazon EC2 EC2-Instance bereit und ist für die Anwendungskonfiguration nützlich. Die Beschränkung der PUT HTTP-Antwort für den Metadaten-Service auf die EC2-Instance schützt das IMDS vor unbefugter Nutzung.

Das TTL-Feld (Time To Live) im IP-Paket wird bei jedem Hop um eins reduziert. Diese Reduzierung kann verwendet werden, um sicherzustellen, dass das Paket nicht außerhalb von EC2 übertragen wird. IMDSv2 schützt EC2-Instances, die möglicherweise als offene Router, Layer-3-Firewalls, VPNs, Tunnel oder NAT-Geräte falsch konfiguriert wurden, wodurch verhindert wird, dass unbefugte Benutzer Metadaten abrufen. Mit IMDSv2 kann die PUT Antwort, die das geheime Token enthält, nicht außerhalb der Instance übertragen werden, da das standardmäßige Hop-Limit für die Beantwortung von Metadaten auf festgelegt ist. 1 Wenn dieser Wert jedoch größer als ist1, kann das Token die EC2-Instance verlassen.

Abhilfe

Informationen zum Ändern des Metadaten-Response-Hop-Limits für eine bestehende Startkonfiguration finden Sie unter Ändern von Instance-Metadaten-Optionen für bestehende Instances im Amazon EC2 EC2-Benutzerhandbuch.

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launch-config-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die zugehörige Startkonfiguration einer Auto Scaling Scaling-Gruppe den Instances der Gruppe eine öffentliche IP-Adresse zuweist. Die Steuerung schlägt fehl, wenn die zugehörige Startkonfiguration eine öffentliche IP-Adresse zuweist.

Amazon EC2 EC2-Instances in einer Auto Scaling Scaling-Gruppenstartkonfiguration sollten keine zugeordnete öffentliche IP-Adresse haben, außer in begrenzten Randfällen. Amazon EC2 EC2-Instances sollten nur hinter einem Load Balancer zugänglich sein, anstatt direkt dem Internet ausgesetzt zu sein.

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration einer Auto-Scaling-Gruppe zu ändern, verwenden Sie eine vorhandene Startkonfiguration als Grundlage

für eine neue Startkonfiguration. Aktualisieren Sie dann die Auto-Scaling-Gruppe so, dass die neue Startkonfiguration verwendet wird. Eine schrittweise Anleitung finden Sie unter Ändern der Startkonfiguration für eine Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. Wählen Sie bei der Erstellung der neuen Startkonfiguration unter Zusätzliche Konfiguration für Erweiterte Details und IP-Adresstyp die Option Keinen Instances eine öffentliche IP-Adresse zuweisen aus.

Nachdem Sie die Startkonfiguration geändert haben, startet Auto Scaling neue Instances mit den neuen Konfigurationsoptionen. Bestehende Instanzen sind nicht betroffen. Um eine bestehende Instance zu aktualisieren, empfehlen wir Ihnen, Ihre Instance zu aktualisieren oder die automatische Skalierung zuzulassen, um ältere Instances auf der Grundlage Ihrer Kündigungsrichtlinien schrittweise durch neuere Instances zu ersetzen. Weitere Informationen zur Aktualisierung von Auto Scaling Scaling-Instances finden Sie unter Auto Scaling Scaling-Instances aktualisieren im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/GV. OC-04.03, CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-multiple-instance-types`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mehrere Instance-Typen verwendet. Die Steuerung schlägt fehl, wenn für die Auto Scaling Scaling-Gruppe nur ein Instanztyp definiert ist.

Sie können die Verfügbarkeit verbessern, indem Sie Ihre Anwendung auf mehreren Instance-Typen bereitstellen, die in mehreren Availability Zones ausgeführt werden. Security Hub CSPM empfiehlt

die Verwendung mehrerer Instanztypen, damit die Auto Scaling Scaling-Gruppe einen anderen Instanztyp starten kann, wenn die Instance-Kapazität in den von Ihnen ausgewählten Availability Zones nicht ausreicht.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit mehreren Instance-Typen finden Sie unter Auto Scaling Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-launch-template`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe anhand einer EC2-Startvorlage erstellt wurde. Diese Steuerung schlägt fehl, wenn eine Amazon EC2 Auto Scaling Scaling-Gruppe nicht mit einer Startvorlage erstellt wird oder wenn keine Startvorlage in einer Richtlinie für gemischte Instanzen angegeben ist.

Eine EC2 Auto Scaling Scaling-Gruppe kann entweder aus einer EC2-Startvorlage oder einer Startkonfiguration erstellt werden. Die Verwendung einer Startvorlage zur Erstellung einer Auto Scaling Scaling-Gruppe stellt jedoch sicher, dass Sie Zugriff auf die neuesten Funktionen und Verbesserungen haben.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit einer EC2-Startvorlage finden Sie unter Erstellen einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage im Amazon EC2 Auto

Scaling Scaling-Benutzerhandbuch. Informationen zum Ersetzen einer Startkonfiguration durch eine Startvorlage finden Sie unter Ersetzen einer Startkonfiguration durch eine Startvorlage im Amazon EC2 EC2-Benutzerhandbuch.

[AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config Regel: `tagged-autoscaling-autoscalinggroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Auto Scaling Scaling-Gruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Auto Scaling Scaling-Gruppe finden Sie unter Tag Auto Scaling Scaling-Gruppen und -Instances im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon ECR

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen des Amazon Elastic Container Registry (Amazon ECR).

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 RA-5, PCI DSS v4.0. 1/63.2.3, PCI DSS v4.0. 1/6.2.4, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: ecr-private-image-scanning-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für ein privates Amazon ECR-Repository das Scannen von Bildern konfiguriert ist. Die Steuerung schlägt fehl, wenn das private ECR-Repository nicht für Scan on Push oder kontinuierliches Scannen konfiguriert ist.

Das Scannen von ECR-Bildern hilft bei der Identifizierung von Softwareschwachstellen in Ihren Container-Images. Die Konfiguration von Bildscans in ECR-Repositorys bietet eine zusätzliche Überprüfungsebene für die Integrität und Sicherheit der gespeicherten Bilder.

Abhilfe

Informationen zum Konfigurieren von Bildscans für ein ECR-Repository finden Sie unter Scannen von Bildern im Amazon Elastic Container Registry User Guide.

[ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8 CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: ecr-private-tag-immutability-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem privaten ECR-Repository die Tag-Unveränderlichkeit aktiviert ist. Diese Kontrolle schlägt fehl, wenn in einem privaten ECR-Repository die Tag-

Unveränderlichkeit deaktiviert ist. Diese Regel gilt, wenn die Tag-Unveränderlichkeit aktiviert ist und den Wert hat. `IMMUTABLE`

Amazon ECR Tag Immutability ermöglicht es Kunden, sich auf die beschreibenden Tags eines Bildes als zuverlässigen Mechanismus zur Nachverfolgung und eindeutigen Identifizierung von Bildern zu verlassen. Ein unveränderliches Tag ist statisch, was bedeutet, dass sich jedes Tag auf ein eindeutiges Bild bezieht. Dies verbessert die Zuverlässigkeit und Skalierbarkeit, da die Verwendung eines statischen Tags immer dazu führt, dass dasselbe Image bereitgestellt wird. Wenn sie konfiguriert ist, verhindert die Unveränderlichkeit von Tags, dass die Tags überschrieben werden, wodurch die Angriffsfläche reduziert wird.

Abhilfe

Informationen zum Erstellen eines Repositorys mit konfigurierten unveränderlichen Tags oder zum Aktualisieren der Image-Tag-Mutabilitätseinstellungen für ein vorhandenes Repository finden Sie unter Image-Tag-Mutability im Amazon Elastic Container Registry-Benutzerhandbuch.

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/ID. AM-08.01, CRI-Profil v2. 2/PR. IR-04.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: ecr-private-lifecycle-policy-configured

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für ein Amazon ECR-Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Diese Kontrolle schlägt fehl, wenn für ein ECR-Repository keine Lebenszyklusrichtlinien konfiguriert sind.

Mit Amazon ECR-Lebenszyklusrichtlinien können Sie das Lebenszyklusmanagement von Images in einem Repository festlegen. Durch die Konfiguration von Lebenszyklusrichtlinien können

Sie die Bereinigung ungenutzter Images und das Verfallsdatum von Images je nach Alter oder Anzahl automatisieren. Durch die Automatisierung dieser Aufgaben können Sie verhindern, dass versehentlich veraltete Bilder in Ihrem Repository verwendet werden.

Abhilfe

Informationen zur Konfiguration einer Lifecycle-Richtlinie finden Sie unter Creating a Lifecycle Policy Preview im Amazon Elastic Container Registry User Guide.

[ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECR::PublicRepository`

AWS Config Regel: `tagged-ecr-publicrepository` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein öffentliches Amazon ECR-Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das öffentliche Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter

`requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das öffentliche Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem öffentlichen ECR-Repository finden Sie unter Tagging an ein öffentliches Amazon ECR-Repository im Amazon Elastic Container Registry-Benutzerhandbuch.

[ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 AU-9

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: ecr-repository-cmk-encryption-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`kmsKeyArns`	Eine Liste der Amazon-Ressourcennamen (ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerelement generiert einen `FAILED` Befund, wenn ein ECR-Repository nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.	StringList (maximal 10 Elemente)	1—10 ARNs vorhandener KMS-Schlüssel. Beispiel: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	Kein Standardwert

Diese Kontrolle prüft, ob ein Amazon ECR-Repository im Ruhezustand verschlüsselt ist und von einem Kunden verwaltet AWS KMS key wird. Die Kontrolle schlägt fehl, wenn das ECR-Repository nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

Standardmäßig verschlüsselt Amazon ECR Repository-Daten mithilfe eines AES-256 Algorithmus mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3). Für zusätzliche Kontrolle können Sie Amazon ECR so konfigurieren, dass die Daten stattdessen mit einem AWS KMS key (SSE-KMS oder DSSE-KMS) verschlüsselt werden. Der KMS-Schlüssel kann sein: ein Von AWS verwalteter Schlüssel ,

den Amazon ECR für Sie erstellt und verwaltet und der den Alias hat`aws/ecr`, oder ein vom Kunden verwalteter Schlüssel, den Sie in Ihrem AWS-Konto erstellen und verwalten. Mit einem vom Kunden verwalteten KMS-Schlüssel haben Sie die volle Kontrolle über den Schlüssel. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels.

> **Note**
>
> AWS KMS unterstützt den kontoübergreifenden Zugriff auf KMS-Schlüssel. Wenn ein ECR-Repository mit einem KMS-Schlüssel verschlüsselt ist, der einem anderen Konto gehört, führt dieses Steuerelement bei der Auswertung des Repositorys keine kontoübergreifenden Prüfungen durch. Die Kontrolle bewertet nicht, ob Amazon ECR auf den Schlüssel zugreifen und ihn verwenden kann, wenn kryptografische Operationen für das Repository ausgeführt werden.

Abhilfe

Sie können die Verschlüsselungseinstellungen für ein vorhandenes ECR-Repository nicht ändern. Sie können jedoch andere Verschlüsselungseinstellungen für ECR-Repositorys angeben, die Sie anschließend erstellen. Amazon ECR unterstützt die Verwendung verschiedener Verschlüsselungseinstellungen für einzelne Repositorys.

Weitere Informationen zu Verschlüsselungsoptionen für ECR-Repositorys finden Sie unter Encryption at rest im Amazon ECR-Benutzerhandbuch. Weitere Informationen zu „Customer Managed AWS KMS keys“ finden Sie AWS KMS keysim Developer Guide.AWS Key Management Service

Security Hub CSPM-Steuerungen für Amazon ECS

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen des Amazon Elastic Container Service (Amazon ECS). Die Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5

SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::Service`

AWS Config Regel: `ecs-service-assign-public-ip-disabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon ECS-Services so konfiguriert sind, dass sie automatisch öffentliche IP-Adressen zuweisen. Diese Steuerung schlägt fehl, wenn dies `AssignPublicIP` der Fall ist`ENABLED`. Diese Kontrolle `AssignPublicIP` ist erfolgreich, falls ja`DISABLED`.

Eine öffentliche IP-Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Amazon ECS-Instances mit einer öffentlichen IP-Adresse starten, sind Ihre Amazon ECS-Instances über das Internet erreichbar. Amazon ECS-Services sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Container-Anwendungsserver ermöglichen kann.

Abhilfe

Zunächst müssen Sie eine Aufgabendefinition für Ihren Cluster erstellen, die den `awsvpc` Netzwerkmodus verwendet und FARGATE für spezifiziert. `requiresCompatibilities` Wählen Sie dann für Compute-Konfiguration die Optionen Starttyp und FARGATE aus. Schalten Sie abschließend für das Feld Netzwerk die Option Öffentliche IP aus, um die automatische Zuweisung öffentlicher IP-Adressen für Ihren Dienst zu deaktivieren.

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/PR. PS-01.09

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-task-definition-pid-mode-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Amazon ECS-Aufgabendefinitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts gemeinsam mit seinen Containern verwenden. Die Steuerung schlägt fehl, wenn die Aufgabendefinition den Prozess-Namespace des Hosts gemeinsam mit den darauf laufenden Containern verwendet. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Ein Prozess-ID-Namespace (PID) sorgt für die Trennung zwischen Prozessen. Er verhindert, dass Systemprozesse sichtbar sind, und ermöglicht die Wiederverwendung von PIDs, einschließlich PID 1. Wenn der PID-Namespace des Hosts gemeinsam mit Containern genutzt wird, könnten Container alle Prozesse auf dem Hostsystem sehen. Dies verringert den Vorteil der Isolierung auf Prozessebene zwischen dem Host und den Containern. Diese Umstände könnten zu unberechtigtem Zugriff auf Prozesse auf dem Host selbst führen, einschließlich der Möglichkeit, diese zu manipulieren und zu beenden. Kunden sollten den Prozess-Namespace des Hosts nicht mit Containern teilen, die darauf laufen.

Abhilfe

Informationen zur Konfiguration der `pidMode` Aufgabendefinition finden Sie unter Aufgabendefinitionsparameter im Amazon Elastic Container Service Developer Guide.

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, CRI Profile v2. 2/PR. AA-05.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-containers-nonprivileged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der `privileged` Parameter in der Container-Definition von Amazon ECS-Aufgabendefinitionen auf gesetzt ist`true`. Die Steuerung schlägt fehl, wenn dieser Parameter gleich ist`true`. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Wir empfehlen, dass Sie erhöhte Rechte aus Ihren ECS-Aufgabendefinitionen entfernen. Wenn der Berechtigungsparameter laute`true`, erhält der Container erhöhte Rechte auf der Host-Container-Instance (ähnlich wie dem Root-Benutzer).

Abhilfe

Informationen zur Konfiguration des `privileged` Parameters für eine Aufgabendefinition finden Sie unter Erweiterte Container-Definitionsparameter im Amazon Elastic Container Service Developer Guide.

[ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-containers-readonly-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in den ECS-Aufgabendefinitionen Container so konfiguriert sind, dass sie nur Lesezugriff auf gemountete Root-Dateisysteme haben. Die Steuerung schlägt fehl, wenn der `readonlyRootFilesystem` Parameter in den Containerdefinitionen der ECS-Aufgabendefinition auf `false` gesetzt ist oder der Parameter in der Containerdefinition innerhalb der Aufgabendefinition nicht vorhanden ist. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Wenn der `readonlyRootFilesystem` Parameter `true` in einer Amazon ECS-Aufgabendefinition auf gesetzt ist, erhält der ECS-Container schreibgeschützten Zugriff auf sein Root-Dateisystem. Dadurch werden Sicherheitsangriffsvektoren reduziert, da das Root-Dateisystem der Container-Instance ohne explizite Volume-Mounts, die über Lese- und Schreibberechtigungen für Dateisystemordner und -verzeichnisse verfügen, nicht manipuliert oder darauf geschrieben werden kann. Die Aktivierung dieser Option entspricht auch dem Prinzip der geringsten Rechte.

> **Note**
>
> Der `readonlyRootFilesystem` Parameter wird für Windows-Container nicht unterstützt. Aufgabendefinitionen, die `runtimePlatform` so konfiguriert sind, dass sie eine `WINDOWS_SERVER` Betriebssystemfamilie angeben, sind als solche gekennzeichnet `NOT_APPLICABLE` und generieren keine Ergebnisse für dieses Steuerelement.

Abhilfe

Um einem Amazon ECS-Container schreibgeschützten Zugriff auf sein Root-Dateisystem zu gewähren, fügen Sie den `readonlyRootFilesystem` Parameter zur Aufgabendefinition für den Container hinzu und setzen Sie den Wert für den Parameter auf. `true` Informationen zu Aufgabendefinitionsparametern und deren Hinzufügen zu einer Aufgabendefinition finden Sie unter Amazon ECS-Aufgabendefinitionen und Aktualisieren einer Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/86.6.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Sichere Entwicklung > Anmeldeinformationen sind nicht fest codiert

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-no-environment-secrets

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:`secretKeys`:`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (nicht anpassbar)

Dieses Steuerelement prüft, ob der Schlüsselwert einer Variablen im `environment` Parameter von ContainerdefinitionenAWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY, oder enthältECS_ENGINE_AUTH_DATA. Dieses Steuerelement schlägt fehl, wenn eine einzelne Umgebungsvariable in einer Containerdefinition gleich `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, oder `ECS_ENGINE_AUTH_DATA` ist. Diese Kontrolle deckt keine Umgebungsvariablen ab, die von anderen Standorten wie Amazon S3 weitergegeben werden. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

AWS Systems Manager Parameter Store kann Ihnen helfen, die Sicherheitslage Ihres Unternehmens zu verbessern. Wir empfehlen, den Parameter Store zum Speichern von Geheimnissen und Anmeldeinformationen zu verwenden, anstatt sie direkt an Ihre Container-Instances zu übergeben oder sie fest in Ihren Code zu codieren.

Abhilfe

Informationen zum Erstellen von Parametern mit SSM finden Sie unter Erstellen von Systems Manager Manager-Parametern im AWS Systems Manager Benutzerhandbuch. Weitere Informationen zum Erstellen einer Aufgabendefinition, die ein Geheimnis spezifiziert, finden Sie unter Spezifying sensitive data using Secrets Manager im Amazon Elastic Container Service Developer Guide.

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: ecs-task-definition-log-configuration

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die letzte aktive Amazon ECS-Aufgabendefinition eine Protokollierungskonfiguration angegeben wurde. Die Steuerung schlägt fehl, wenn für die Aufgabendefinition die `logConfiguration` Eigenschaft nicht definiert `logDriver` ist oder wenn der Wert für in mindestens einer Containerdefinition Null ist.

Die Protokollierung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS aufrechtzuerhalten. Das Sammeln von Daten aus Aufgabendefinitionen bietet Transparenz, was Ihnen helfen kann, Prozesse zu debuggen und die Ursache von Fehlern zu finden. Wenn Sie eine Protokollierungslösung verwenden, die nicht in der ECS-Aufgabendefinition definiert werden muss (z. B. eine Protokollierungslösung eines Drittanbieters), können Sie diese Steuerung deaktivieren, nachdem Sie sichergestellt haben, dass Ihre Protokolle ordnungsgemäß erfasst und übermittelt wurden.

Abhilfe

Informationen zum Definieren einer Protokollkonfiguration für Ihre Amazon ECS-Aufgabendefinitionen finden Sie unter Angeben einer Protokollkonfiguration in Ihrer Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

[ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::Service`

AWS Config -Regel: ecs-fargate-latest-platform-version

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `latestLinuxVersion: 1.4.0`(nicht anpassbar)
- `latestWindowsVersion: 1.0.0`(nicht anpassbar)

Dieses Steuerelement prüft, ob die Amazon ECS Fargate-Dienste die neueste Version der Fargate-Plattform ausführen. Diese Steuerung schlägt fehl, wenn die Plattformversion nicht die neueste ist.

AWS Fargate Plattformversionen beziehen sich auf eine spezifische Laufzeitumgebung für die Fargate-Task-Infrastruktur, bei der es sich um eine Kombination aus Kernel- und Container-Laufzeitversionen handelt. Neue Plattformversionen werden veröffentlicht, wenn sich die Laufzeitumgebung weiterentwickelt. Beispielsweise kann eine neue Version für Kernel- oder Betriebssystemupdates, neue Funktionen, Bugfixes oder Sicherheitsupdates veröffentlicht werden. Sicherheits-Updates und -Patches für Ihre -Fargate-Aufgaben werden automatisch bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das sich auf eine Plattformversion auswirkt, wird die AWS Plattformversion gepatcht.

Abhilfe

Informationen zum Aktualisieren eines vorhandenen Service, einschließlich seiner Plattformversion, finden Sie unter Aktualisieren eines Service im Amazon Elastic Container Service Developer Guide.

[ECS.12] ECS-Cluster sollten Container Insights verwenden

Verwandte Anforderungen: NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, CRI Profile v2. 2/PR. IR-04.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::Cluster`

AWS Config -Regel: ecs-container-insights-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ECS-Cluster Container Insights verwenden. Diese Steuerung schlägt fehl, wenn Container Insights nicht für einen Cluster eingerichtet ist.

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS-Clustern. Verwenden Sie CloudWatch Container Insights, um Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zu sammeln, zu aggregieren und zusammenzufassen. CloudWatch sammelt automatisch Metriken für viele Ressourcen wie CPU, Arbeitsspeicher, Festplatte und Netzwerk. Container Insights bietet auch Diagnoseinformationen, wie z. B.Fehler beim Container-Neustart, damit Sie Probleme schnell aufdecken und beheben können. Sie können auch CloudWatch Alarme für Metriken einrichten, die Container Insights sammelt.

Abhilfe

Informationen zur Verwendung von Container Insights finden Sie unter Service aktualisieren im CloudWatch Amazon-Benutzerhandbuch.

[ECS.13] ECS-Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Service`

AWS Config Regel: `tagged-ecs-service` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Service Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Dienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Service finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

[ECS.14] ECS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Cluster`

AWS Config Regel: `tagged-ecs-cluster` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Cluster finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

[ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: `tagged-ecs-taskdefinition` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon ECS-Aufgabendefinition Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Aufgabendefinition keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Aufgabendefinition mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer ECS-Aufgabendefinition finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen

Verwandte Anforderungen: PCI DSS v4.0. 1/14.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskSet`

AWS Config Regel: `ecs-taskset-assign-public-ip-disabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon ECS-Task-Set so konfiguriert ist, dass öffentliche IP-Adressen automatisch zugewiesen werden. Die Steuerung schlägt fehl, wenn sie auf gesetzt `AssignPublicIP` ist`ENABLED`.

Eine öffentliche IP-Adresse ist über das Internet erreichbar. Wenn Sie Ihr Task-Set mit einer öffentlichen IP-Adresse konfigurieren, können die mit dem Task-Set verknüpften Ressourcen über das Internet erreicht werden. ECS-Aufgabensätze sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Container-Anwendungsserver ermöglichen kann.

Abhilfe

Informationen zum Aktualisieren eines ECS-Aufgabensatzes, sodass er keine öffentliche IP-Adresse verwendet, finden Sie unter Aktualisieren einer Amazon ECS-Aufgabendefinition mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.

[ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-task-definition-network-mode-not-host

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die letzte aktive Revision einer Amazon ECS-Aufgabendefinition den `host` Netzwerkmodus verwendet. Die Steuerung schlägt fehl, wenn die letzte aktive Revision der ECS-Aufgabendefinition den `host` Netzwerkmodus verwendet.

Bei Verwendung des `host` Netzwerkmodus ist das Netzwerk eines Amazon ECS-Containers direkt an den zugrunde liegenden Host gebunden, auf dem der Container ausgeführt wird. Folglich ermöglicht dieser Modus Containern, sich mit privaten Loopback-Netzwerkdiensten auf dem Host zu verbinden und sich als der Host auszugeben. Weitere wichtige Nachteile bestehen darin, dass es im `host` Netzwerkmodus keine Möglichkeit gibt, einen Container-Port neu zuzuordnen, und dass Sie nicht mehr als eine einzige Instanziierung einer Aufgabe auf jedem Host ausführen können.

Abhilfe

Informationen zu Netzwerkmodi und Optionen für Amazon ECS-Aufgaben, die auf Amazon EC2 EC2-Instances gehostet werden, finden Sie unter Netzwerkoptionen für Amazon ECS-Aufgaben für den EC2-Starttyp im Amazon Elastic Container Service Developer Guide. Informationen zum Erstellen einer neuen Version einer Aufgabendefinition und zum Angeben eines anderen Netzwerkmodus finden Sie in diesem Handbuch unter Aktualisieren einer Amazon ECS-Aufgabendefinition.

Wenn die Amazon ECS-Aufgabendefinition von erstellt wurde AWS Batch, finden Sie unter Netzwerkmodi für AWS Batch Jobs Informationen zu Netzwerkmodi und zur typischen Verwendung von AWS Batch Auftragstypen sowie zur Auswahl einer sicheren Option.

[ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden

Kategorie: Schützen > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-task-definition-efs-encryption-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die letzte aktive Version einer Amazon ECS-Aufgabendefinition die Verschlüsselung während der Übertragung für EFS-Volumes verwendet. Die Steuerung schlägt fehl, wenn in der letzten aktiven Version der ECS-Aufgabendefinition die Verschlüsselung während der Übertragung für EFS-Volumes deaktiviert ist.

Amazon EFS-Volumes bieten einfachen, skalierbaren und dauerhaften gemeinsamen Dateispeicher für Ihre Amazon ECS-Aufgaben. Amazon EFS unterstützt die Verschlüsselung von Daten während der Übertragung mit Transport Layer Security (TLS). Wenn die Verschlüsselung von Daten während der Übertragung als Mount-Option für Ihr EFS-Dateisystem deklariert ist, stellt Amazon EFS beim Mounten Ihres Dateisystems eine sichere TLS-Verbindung mit Ihrem EFS-Dateisystem her.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung während der Übertragung für Amazon ECS-Aufgabendefinitionen mit EFS-Volumes finden Sie unter Schritt 5: Erstellen einer Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

[ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben

Kategorie: Schützen > Datenschutz

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::CapacityProvider`

AWS Config -Regel: ecs-capacity-provider-termination-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon ECS-Kapazitätsanbieter den Managed Termination Protection aktiviert hat. Die Kontrolle schlägt fehl, wenn der verwaltete Kündigungsschutz bei einem ECS-Kapazitätsanbieter nicht aktiviert ist.

Amazon-ECS-Kapazitätsanbieter verwalten die Skalierung der Infrastruktur für Aufgaben in Ihren Clustern. Wenn Sie EC2-Instances für Ihre Kapazität verwenden, verwenden Sie die Auto-Scaling-Gruppe, um die EC2-Instances zu verwalten. Mit dem verwalteten Beendigungsschutz kann das Cluster-Auto-Scaling steuern, welche Instances beendet werden. Wenn Sie den verwalteten Beendigungsschutz verwenden, beendet Amazon ECS nur EC2-Instances, auf denen keine Amazon-ECS-Aufgaben ausgeführt werden.

> **Note**
>
> Bei Verwendung des verwalteten Beendigungsschutzes muss auch die verwaltete Skalierung verwendet werden, da andernfalls der verwaltete Beendigungsschutz nicht funktioniert.

Abhilfe

Informationen zum Aktivieren des Managed Termination Protection für einen Amazon ECS-Kapazitätsanbieter finden Sie unter Aktualisierung des Managed Termination Protection for Amazon ECS Capacity Providers im Amazon Elastic Container Service Developer Guide.

[ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-task-definition-linux-user-non-root

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die letzte aktive Revision einer Amazon ECS-Aufgabendefinition Linux-Container so konfiguriert, dass sie als Nicht-Root-Benutzer ausgeführt werden. Die Steuerung schlägt fehl, wenn ein standardmäßiger Root-Benutzer konfiguriert ist oder eine Benutzerkonfiguration für einen Container fehlt.

Wenn Linux-Container mit Root-Rechten ausgeführt werden, stellen sie mehrere erhebliche Sicherheitsrisiken dar. Root-Benutzer haben uneingeschränkten Zugriff auf den Container. Dieser erhöhte Zugriff erhöht das Risiko von Container-Escape-Angriffen, bei denen ein Angreifer möglicherweise aus der Container-Isolation ausbrechen und auf das zugrunde liegende Hostsystem zugreifen könnte. Wenn ein Container, der als Root läuft, kompromittiert ist, können Angreifer dies ausnutzen, um auf Ressourcen des Hostsystems zuzugreifen oder diese zu ändern, was sich auf andere Container oder den Host selbst auswirkt. Darüber hinaus könnte der Root-Zugriff Angriffe zur Eskalation von Rechten ermöglichen, sodass Angreifer zusätzliche Berechtigungen erlangen

können, die über den vorgesehenen Umfang des Containers hinausgehen. Der Benutzerparameter in ECS-Aufgabendefinitionen kann Benutzer in verschiedenen Formaten angeben, darunter Benutzername, Benutzer-ID, Benutzername mit Gruppe oder UID mit Gruppen-ID. Es ist wichtig, sich bei der Konfiguration von Aufgabendefinitionen dieser verschiedenen Formate bewusst zu sein, um sicherzustellen, dass kein Root-Zugriff versehentlich gewährt wird. Gemäß dem Prinzip der geringsten Rechte sollten Container mit den erforderlichen Mindestberechtigungen ausgeführt werden und Benutzer verwenden, die keine Root-Benutzer sind. Dieser Ansatz reduziert die potenzielle Angriffsfläche erheblich und mindert die Auswirkungen potenzieller Sicherheitsverletzungen.

> **Note**
>
> Dieses Steuerelement wertet die Containerdefinitionen in einer Aufgabendefinition nur dann aus, wenn die in der Aufgabendefinition als konfiguriert `operatingSystemFamily` `operatingSystemFamily` ist `LINUX` oder nicht. Das Steuerelement generiert ein `FAILED` Ergebnis für eine ausgewertete Aufgabendefinition, wenn eine Containerdefinition in der Aufgabendefinition `user` nicht als Standard-Root-Benutzer `user` konfiguriert oder konfiguriert wurde. Die Standard-Root-Benutzer für `LINUX` Container sind `"root"` und`"0"`.

Abhilfe

Informationen zum Erstellen einer neuen Version einer Amazon ECS-Aufgabendefinition und zum Aktualisieren des `user` Parameters in der Container-Definition finden Sie unter Aktualisieren einer Amazon ECS-Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

[ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: ecs-task-definition-windows-user-non-admin

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die letzte aktive Revision einer Amazon ECS-Aufgabendefinition Windows-Container so konfiguriert, dass sie als Benutzer ausgeführt werden, die keine Standardadministratoren sind. Die Steuerung schlägt fehl, wenn ein Standardadministrator als Benutzer konfiguriert ist oder wenn keine Benutzerkonfiguration für einen Container vorhanden ist.

Wenn Windows-Container mit Administratorrechten ausgeführt werden, stellen sie mehrere erhebliche Sicherheitsrisiken dar. Administratoren haben uneingeschränkten Zugriff auf den Container. Dieser erhöhte Zugriff erhöht das Risiko von Container-Escape-Angriffen, bei denen ein Angreifer möglicherweise aus der Container-Isolation ausbrechen und auf das zugrunde liegende Hostsystem zugreifen könnte.

> **Note**
>
> Dieses Steuerelement wertet die Containerdefinitionen in einer Aufgabendefinition nur dann aus, wenn das in der Aufgabendefinition als konfiguriert `operatingSystemFamily` `operatingSystemFamily` ist `WINDOWS_SERVER` oder nicht. Das Steuerelement generiert einen `FAILED` Befund für eine ausgewertete Aufgabendefinition, wenn eine Containerdefinition in der Aufgabendefinition `user` nicht als Standardadministrator für `WINDOWS_SERVER` Container `user` konfiguriert oder konfiguriert wurde. `"containeradministrator"`

Abhilfe

Informationen zum Erstellen einer neuen Version einer Amazon ECS-Aufgabendefinition und zum Aktualisieren des `user` Parameters in der Container-Definition finden Sie unter Aktualisieren einer Amazon ECS-Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

Security Hub CSPM-Steuerelemente für Amazon EFS

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen des Amazon Elastic File System (Amazon EFS). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/23.3.1, Benchmark v3.0 für CIS AWS Foundations. 0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5

SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: efs-encrypted-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System so konfiguriert ist, dass es die Dateidaten verschlüsselt mit AWS KMS. Die Prüfung schlägt in den folgenden Fällen fehl.

- `Encrypted`ist `false` in der `DescribeFileSystems`Antwort auf eingestellt.
- Der `KmsKeyId`-Schlüssel in der `DescribeFileSystems`-Antwort stimmt nicht mit dem `KmsKeyId`-Parameter für `efs-encrypted-check` überein.

Beachten Sie, dass dieses Steuerelement den `KmsKeyId`-Parameter nicht für `efs-encrypted-check` verwendet. Es überprüft nur den Wert von `Encrypted`.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in Amazon EFS sollten Sie verschlüsselte Dateisysteme erstellen. Amazon EFS unterstützt die Verschlüsselung von Dateisystemen im Ruhezustand. Sie können die Verschlüsselung von Daten im Ruhezustand aktivieren, wenn Sie ein Amazon EFS-Dateisystem erstellen. Weitere Informationen zur Amazon EFS-Verschlüsselung finden Sie unter Datenverschlüsselung in Amazon EFS im Amazon Elastic File System-Benutzerhandbuch.

Abhilfe

Einzelheiten zur Verschlüsselung eines neuen Amazon EFS-Dateisystems finden Sie unter Verschlüsseln ruhender Daten im Amazon Elastic File System-Benutzerhandbuch.

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. DS-11.01

Kategorie: Wiederherstellung > Resilienz > Backup

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: efs-in-backup-plan

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System (Amazon EFS) -Dateisysteme zu den Sicherungsplänen in hinzugefügt wurden AWS Backup. Die Kontrolle schlägt fehl, wenn Amazon EFS-Dateisysteme nicht in den Backup-Plänen enthalten sind.

Die Einbeziehung von EFS-Dateisystemen in die Backup-Pläne hilft Ihnen, Ihre Daten vor Löschung und Datenverlust zu schützen.

Abhilfe

Informationen zum Aktivieren automatischer Backups für ein vorhandenes Amazon EFS-Dateisystem finden Sie unter Erste Schritte 4: Automatische Amazon EFS-Backups erstellen im AWS Backup Entwicklerhandbuch.

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

Verwandte Anforderungen: NIST.800-53.r5 AC-6 (10), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config -Regel: efs-access-point-enforce-root-directory

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS-Zugriffspunkte so konfiguriert sind, dass sie ein Stammverzeichnis erzwingen. Die Steuerung schlägt fehl, wenn der `Path` Wert von auf `/` (das Standard-Stammverzeichnis des Dateisystems) gesetzt ist.

Wenn Sie ein Stammverzeichnis erzwingen, verwendet der NFS-Client, der den Zugriffspunkt verwendet, das auf dem Zugriffspunkt konfigurierte Stammverzeichnis anstelle des Stammverzeichnisses des Dateisystems. Durch die Festlegung eines Stammverzeichnisses für einen Access Point wird der Datenzugriff eingeschränkt, da sichergestellt wird, dass Benutzer des Access Points nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Abhilfe

Anweisungen zum Erzwingen eines Stammverzeichnisses für einen Amazon EFS-Zugriffspunkt finden Sie unter Erzwingen eines Stammverzeichnisses mit einem Zugriffspunkt im Amazon Elastic File System-Benutzerhandbuch.

[EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen

Verwandte Anforderungen: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0. 1/73.3.1, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-10.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config -Regel: efs-access-point-enforce-user-identity

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS Access Points so konfiguriert sind, dass sie eine Benutzeridentität erzwingen. Diese Steuerung schlägt fehl, wenn beim Erstellen des EFS-Zugriffspunkts keine POSIX-Benutzeridentität definiert wurde.

Amazon-EFS-Zugangspunkte sind anwendungsspezifische Einstiegspunkte in ein EFS-Dateisystem, die das Verwalten des Anwendungszugriffs auf freigegebene Datensätze erleichtern. Zugangspunkte können eine Benutzeridentität, einschließlich der POSIX-Gruppen des Benutzers, für alle Dateisystemanforderungen erzwingen, die über den Zugangspunkt erfolgen. Zugriffspunkte können

auch ein anderes Stammverzeichnis für das Dateisystem erzwingen, so dass Clients nur auf Daten im angegebenen Verzeichnis oder in seinen Unterverzeichnissen zugreifen können.

Abhilfe

Informationen zur Durchsetzung einer Benutzeridentität für einen Amazon EFS Access Point finden Sie unter Durchsetzung einer Benutzeridentität mithilfe eines Access Points im Amazon Elastic File System-Benutzerhandbuch.

[EFS.5] EFS-Zugangspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config Regel: `tagged-efs-accesspoint` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EFS-Zugriffspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn der Access Point keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter angegebenen Schlüssel verfügt`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn

der Access Point mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EFS-Zugangspunkt finden Sie unter Tagging Amazon EFS-Ressourcen im Amazon Elastic File System-Benutzerhandbuch.

[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen

Verwandte Anforderungen: NIST.800-53.r5 SC-7, NIST.800-171.r2 3.1.20, PCI DSS v4.0. 1/13.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Netzwerksicherheit > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: efs-mount-target-public-accessible

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EFS-Mount-Ziel Subnetzen zugeordnet ist, die beim Start öffentliche IP-Adressen zuweisen. Die Steuerung schlägt fehl, wenn das Mount-Ziel Subnetzen zugeordnet ist, die beim Start öffentliche IP-Adressen zuweisen.

Subnetze verfügen über Attribute, die bestimmen, ob im Subnetz erstellte Netzwerkschnittstellen automatisch öffentliche IP-Adressen erhalten. Für IPv4 ist das `MapPublicIpOnLaunch` Attribut auf für Standard-Subnetze und `TRUE` für nicht standardmäßige Subnetze gesetzt (mit einer Ausnahme `FALSE` für nicht standardmäßige Subnetze, die mit dem EC2 Launch Instance Wizard erstellt wurden, wo es auf gesetzt ist). `TRUE` Für IPv6 ist das `AssignIpv6AddressOnCreation` Attribut standardmäßig auf für alle Subnetze gesetzt. `FALSE`

Amazon EFS-Mount-Zielen können zwar keine öffentlichen IPv4-Adressen zugewiesen werden, aber ihre Platzierung in Subnetzen, die so konfiguriert sind, dass beim Start öffentliche IP-Adressen zugewiesen werden, deutet darauf hin, dass gemeinsam genutzte Instances, die in solchen Subnetzen gestartet werden, die möglicherweise das EFS-Dateisystem mounten, automatisch öffentliche IP-Adressen erhalten, wodurch das Risiko besteht, dass die Dateisystemdaten von öffentlich adressierten Hosts aus zugänglich werden.

Mount-Ziele in Subnetzen mit aktivierter automatischer Zuweisung von öffentlichen IPv6-Adressen können global routbare IPv6-Adressen empfangen.

> **Note**
>
> Am 3. August 2026 hat Security Hub CSPM diese Kontrolle aus dem Standard AWS Foundational Security Best Practices (FSBP) entfernt. Dieses Steuerelement wird im Standard NIST SP 800-53 Rev. 5, im Standard NIST SP 800-171 Revision 2 und im Standard PCI DSS v4.0.1 verfügbar sein.

Abhilfe

Um ein vorhandenes Mount-Ziel einem anderen Subnetz zuzuordnen, müssen Sie ein neues Mount-Ziel in einem Subnetz erstellen, das beim Start keine öffentlichen IP-Adressen zuweist, und dann das alte Mount-Ziel entfernen. Informationen zur Verwaltung von Mount-Zielen finden Sie unter

Erstellen und Verwalten von Mount-Zielen und Sicherheitsgruppen im Amazon Elastic File System-Benutzerhandbuch.

[EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein

Verwandte Anforderungen: CRI Profile v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::EFS::FileSystem`

AWS Config -Regel: efs-automatic-backups-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für ein Amazon EFS-Dateisystem automatische Backups aktiviert sind. Diese Steuerung schlägt fehl, wenn für das EFS-Dateisystem keine automatischen Backups aktiviert sind.

Eine Datensicherung ist eine Kopie Ihrer System-, Konfiguration- oder Anwendungsdaten, die getrennt vom Original gespeichert wird. Durch die Aktivierung regelmäßiger Backups können Sie wertvolle Daten vor unvorhergesehenen Ereignissen wie Systemausfällen, Cyberangriffen oder versehentlichem Löschen schützen. Eine robuste Backup-Strategie ermöglicht auch eine schnellere Wiederherstellung, einen unterbrechungsfreien Betrieb und sorgt für mehr Sicherheit angesichts potenzieller Datenverluste.

Abhilfe

Informationen AWS Backup zur Verwendung von EFS-Dateisystemen finden Sie unter Sicherung von EFS-Dateisystemen im Amazon Elastic File System-Benutzerhandbuch.

[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/23.3.1, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: efs-filesystem-ct-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EFS-Dateisystem Daten mit AWS Key Management Service (AWS KMS) verschlüsselt. Die Steuerung schlägt fehl, wenn ein Dateisystem nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Aktivieren der Verschlüsselung im Ruhezustand für ein neues EFS-Dateisystem finden Sie unter Verschlüsseln von Daten im Ruhezustand im Amazon Elastic File System-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon EKS

Diese Security Hub CSPM-Steuerungen bewerten den Service und die Ressourcen des Amazon Elastic Kubernetes Service (Amazon EKS). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.05

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: eks-endpoint-no-public-access

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster-Endpunkt öffentlich zugänglich ist. Die Kontrolle schlägt fehl, wenn ein EKS-Cluster über einen öffentlich zugänglichen Endpunkt verfügt.

Wenn Sie einen neuen Cluster erstellen, erstellt Amazon EKS einen Endpunkt für den verwalteten Kubernetes-API-Server, den Sie für die Kommunikation mit Ihrem Cluster verwenden. Standardmäßig ist dieser API-Server-Endpunkt öffentlich im Internet verfügbar. Der Zugriff auf den API-Server wird durch eine Kombination aus AWS Identity and Access Management (IAM) und nativer Kubernetes-Rollenbasierter Zugriffskontrolle (RBAC) gesichert. Indem Sie den öffentlichen Zugriff auf den Endpunkt unterbinden, können Sie verhindern, dass Ihr Cluster unbeabsichtigt gefährdet ist und Sie darauf zugreifen können.

Abhilfe

Informationen zum Ändern des Endpunktzugriffs für einen vorhandenen EKS-Cluster finden Sie unter Ändern des Cluster-Endpunktzugriffs im Amazon EKS-Benutzerhandbuch. Sie können den Endpunktzugriff für einen neuen EKS-Cluster einrichten, wenn Sie ihn erstellen. Anweisungen zum Erstellen eines neuen Amazon EKS-Clusters finden Sie unter Erstellen eines Amazon EKS-Clusters im Amazon EKS-Benutzerhandbuch.

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/123.3.4, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: eks-cluster-supported-version

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `oldestVersionSupported`: `1.34` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer Kubernetes-Version mit Standardunterstützung ausgeführt wird. Die Steuerung schlägt fehl, wenn der Amazon EKS-Cluster auf einer nicht unterstützten Version oder Version mit erweitertem Support ausgeführt wird.

Wenn Ihre Anwendung keine bestimmte Version von Kubernetes benötigt, empfehlen wir Ihnen, die neueste verfügbare Kubernetes-Version zu verwenden, die von EKS für Ihre Cluster unterstützt wird. Weitere Informationen finden Sie im Amazon EKS Kubernetes-Release-Kalender und Understand the Kubernetes Version Lifecycle on Amazon EKS im Amazon EKS-Benutzerhandbuch.

Abhilfe

Informationen zum Aktualisieren eines EKS-Clusters finden Sie unter Aktualisieren eines vorhandenen Clusters auf eine neue Kubernetes-Version im Amazon EKS-Benutzerhandbuch.

[EKS.6] EKS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::Cluster`

AWS Config Regel: `tagged-eks-cluster` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EKS-Cluster finden Sie unter Taggen Ihrer Amazon EKS-Ressourcen im Amazon EKS-Benutzerhandbuch.

[EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::IdentityProviderConfig`

AWS Config Regel: `tagged-eks-identityproviderconfig` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EKS-Identitätsanbieter-Konfiguration Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Konfiguration keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Konfiguration mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu Konfigurationen eines EKS-Identitätsanbieters finden Sie unter Taggen Ihrer Amazon EKS-Ressourcen im Amazon EKS-Benutzerhandbuch.

[EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (7), NIST.800-53.r5 AU-9 (9), (8) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: eks-cluster-log-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `logTypes: audit`(nicht anpassbar)

Dieses Steuerelement prüft, ob für einen Amazon EKS-Cluster die Auditprotokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Audit-Protokollierung für den Cluster nicht aktiviert ist.

> **Note**
>
> Dieses Steuerelement überprüft nicht, ob die Amazon EKS-Auditprotokollierung über Amazon Security Lake für aktiviert ist AWS-Konto.

Die EKS-Protokollierung auf der Kontrollebene stellt Prüf- und Diagnoseprotokolle direkt von der EKS-Steuerebene zu Amazon CloudWatch Logs in Ihrem Konto bereit. Sie können die Protokolltypen auswählen, die Sie benötigen, und die Protokolle werden als Protokollstreams an eine Gruppe für jeden EKS-Cluster gesendet CloudWatch. Die Protokollierung bietet Einblick in den Zugriff und die Leistung von EKS-Clustern. Indem Sie die Protokolle der EKS-Kontrollebene für Ihre EKS-Cluster an CloudWatch Logs senden, können Sie Vorgänge zu Prüf- und Diagnosezwecken an einem zentralen Ort aufzeichnen.

Abhilfe

Informationen zum Aktivieren von Audit-Logs für Ihren EKS-Cluster finden Sie unter Aktivieren und Deaktivieren von Control Plane-Protokollen im Amazon EKS-Benutzerhandbuch.

[EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Nodegroup`

AWS Config -Regel: eks-nodegroup-supported-version-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `oldestVersionSupported`: `1.34` (nicht anpassbar)

Dieses Steuerelement prüft, ob eine Amazon EKS-Knotengruppe auf einer Kubernetes-Version mit Standardunterstützung ausgeführt wird. Die Steuerung schlägt fehl, wenn die Amazon EKS-Knotengruppe auf einer nicht unterstützten Version oder Version mit erweitertem Support ausgeführt wird.

Nur Kubernetes-Versionen mit Standardunterstützung erhalten den vollständigen Satz an Sicherheitspatches, Bugfixes und Sicherheitsfunktionen. Versionen mit erweitertem Support erhalten Patches für kritische und wichtige Sicherheitslücken, aber sie erhalten keine Patches für Sicherheitslücken mit geringerem Schweregrad, nicht sicherheitsrelevante Bugfixes oder Sicherheitsfunktionen, die in neueren Kubernetes-Versionen eingeführt wurden. Amazon EKS aktualisiert Knotengruppen nicht automatisch, sodass Patches auf Knotenebene erst angewendet werden, nachdem Sie Ihre Knotengruppen aktualisiert haben, um die neuesten für Amazon EKS optimierten AMIs zu verwenden. Versionen, die das Ende des erweiterten Supports hinter sich haben, erhalten keine Sicherheitspatches, Bugfixes oder Kompatibilitätsupdates mehr von. AWS Nicht unterstützte Versionen können bekannte Sicherheitslücken enthalten, die in neueren Versionen behoben wurden, und es kann zu Kompatibilitätsproblemen mit aktualisierten AWS-Services Container-Images und Drittanbieter-Tools im Kubernetes-Ökosystem kommen. Wenn Ihre Anwendung keine bestimmte Version von Kubernetes benötigt, empfehlen wir Ihnen, die neueste verfügbare Kubernetes-Version zu verwenden, die von Amazon EKS für Ihre Knotengruppen unterstützt wird. Weitere Informationen finden Sie im Amazon EKS Kubernetes-Veröffentlichungskalender und im Amazon EKS-Benutzerhandbuch im Überblick über jede Phase von Knotenaktualisierungen.

Abhilfe

Informationen zum Aktualisieren einer EKS-Knotengruppe finden Sie unter Aktualisieren einer verwalteten Knotengruppe für Ihren Cluster im Amazon EKS-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für ElastiCache

Diese AWS Security Hub CSPM Kontrollen bewerten den ElastiCache Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Hoch

Ressourcentyp:`AWS::ElastiCache::CacheCluster`, `AWS:ElastiCache:ReplicationGroup`

AWS Config -Regel: elasticache-redis-cluster-automatic-backup-check

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`snapshotRetentionPeriod`	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	1 auf 35	1

Dieses Steuerelement bewertet, ob für einen Amazon ElastiCache (Redis OSS) -Cluster automatische Backups aktiviert sind. Die Steuerung schlägt fehl, wenn der `SnapshotRetentionLimit` für den Redis OSS-Cluster angegebene Zeitraum kürzer als der angegebene Zeitraum ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub CSPM einen Standardwert von 1 Tag.

ElastiCache (Redis OSS) -Cluster können ihre Daten sichern. Sie können das Backup verwenden, um einen Cluster wiederherzustellen oder einen neuen Cluster zu starten. Das Backup besteht aus den Metadaten des Clusters sowie allen Daten im Cluster. Alle Backups werden auf Amazon S3 geschrieben, was dauerhaften Speicherplatz bietet. Sie können Ihre Daten wiederherstellen, indem Sie einen neuen ElastiCache Cluster erstellen und ihn mit Daten aus einem Backup füllen.

Sie können Backups mithilfe der AWS-Managementkonsole AWS CLI, und der ElastiCache API verwalten.

> **Note**
>
> Dieses Steuerelement bewertet auch ElastiCache Replikationsgruppen (Redis OSS und Valkey).

Abhilfe

Informationen zur Planung automatischer Backups für einen ElastiCache Cluster finden Sie unter Automatische Backups planen im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ElastiCache::CacheCluster`

AWS Config -Regel: elasticache-auto-minor-version-upgrade-check

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle bewertet, ob Amazon ElastiCache automatisch kleinere Versions-Upgrades auf einen Cache-Cluster anwendet. Die Kontrolle schlägt fehl, wenn auf den Cache-Cluster keine automatischen Upgrades für Nebenversionen angewendet werden.

> **Note**
>
> Diese Steuerung gilt nicht für ElastiCache Memcached-Cluster.

Das automatische Upgrade von Nebenversionen ist eine Funktion, die Sie in Amazon aktivieren können ElastiCache , um Ihre Cache-Cluster automatisch zu aktualisieren, wenn eine neue kleinere Cache-Engine-Version verfügbar ist. Diese Upgrades können Sicherheitspatches und Bugfixes beinhalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Abhilfe

Informationen zum automatischen Anwenden kleinerer Versions-Upgrades auf einen vorhandenen ElastiCache Cache-Cluster finden Sie unter Versionsverwaltung für ElastiCache im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02, CRI-Profil v2. 2/RC. RP-01.01

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: elasticache-repl-grp-auto-failover-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für eine ElastiCache Replikationsgruppe das automatische Failover aktiviert ist. Die Steuerung schlägt fehl, wenn der automatische Failover für eine Replikationsgruppe nicht aktiviert ist.

Wenn der automatische Failover für eine Replikationsgruppe aktiviert ist, erfolgt für die Rolle des Primärknotens automatisch ein Failover auf eine der Read Replicas. Dieses Failover und die Replikatheraufstufung stellen sicher, dass Sie nach Abschluss der Heraufstufung wieder auf den neuen Primärserver schreiben können, wodurch die Gesamtausfallzeit im Falle eines Fehlers reduziert wird.

Abhilfe

Informationen zum Aktivieren des automatischen Failovers für eine bestehende ElastiCache Replikationsgruppe finden Sie unter Modifizieren eines ElastiCache Clusters im ElastiCache Amazon-Benutzerhandbuch. Wenn Sie die ElastiCache Konsole verwenden, setzen Sie Auto Failover auf aktiviert.

[ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: elasticache-repl-grp-encrypted-at-rest

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine ElastiCache Replikationsgruppe im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Replikationsgruppe im Ruhezustand nicht verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. ElastiCache (Redis OSS) Replikationsgruppen sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung im Ruhezustand für eine ElastiCache Replikationsgruppe finden Sie unter Enabling at rest encryption im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23,

NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: elasticache-repl-grp-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine ElastiCache Replikationsgruppe während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Replikationsgruppe bei der Übertragung nicht verschlüsselt wird.

Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann. Wenn Sie die Verschlüsselung bei der Übertragung in einer ElastiCache Replikationsgruppe aktivieren, werden Ihre Daten immer dann verschlüsselt, wenn sie von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung während der Übertragung für eine ElastiCache Replikationsgruppe finden Sie unter Aktivieren der Verschlüsselung bei der Übertragung im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/83.3.1, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: elasticache-repl-grp-redis-auth-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Replikationsgruppe ElastiCache (Redis OSS) Redis OSS AUTH aktiviert ist. Die Steuerung schlägt fehl, wenn die Redis OSS-Version der Replikationsgruppenknoten unter 6.0 liegt und `AuthToken` nicht verwendet wird.

Wenn Sie Redis-Authentifizierungstoken oder Passwörter verwenden, benötigt Redis ein Passwort, bevor Clients Befehle ausführen können, was die Datensicherheit verbessert. Für Redis 6.0 und spätere Versionen empfehlen wir die Verwendung von Role-Based Access Control (RBAC). Da RBAC für Redis-Versionen vor 6.0 nicht unterstützt wird, wertet dieses Steuerelement nur Versionen aus, die die RBAC-Funktion nicht verwenden können.

Abhilfe

Informationen zur Verwendung von Redis AUTH in einer ElastiCache (Redis OSS) Replikationsgruppe finden Sie unter Ändern des AUTH-Tokens auf einem vorhandenen ElastiCache (Redis OSS) -Cluster im Amazon-Benutzerhandbuch. ElastiCache

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), CRI Profile v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::ElastiCache::CacheCluster`

AWS Config -Regel: elasticache-subnet-group-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein ElastiCache Cluster mit einer benutzerdefinierten Subnetzgruppe konfiguriert ist. Die Steuerung schlägt fehl, wenn `CacheSubnetGroupName` für einen ElastiCache Cluster der Wert `default` gilt.

Beim Starten eines ElastiCache Clusters wird eine Standard-Subnetzgruppe erstellt, falls noch keine vorhanden ist. Die Standardgruppe verwendet Subnetze aus der standardmäßigen Virtual Private Cloud (VPC). Wir empfehlen, benutzerdefinierte Subnetzgruppen zu verwenden, die die Subnetze, in denen sich der Cluster befindet, und die Netzwerke, die der Cluster von den Subnetzen erbt, restriktiver behandeln.

Abhilfe

Informationen zum Erstellen einer neuen Subnetzgruppe für einen ElastiCache Cluster finden Sie unter Erstellen einer Subnetzgruppe im ElastiCache Amazon-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Elastic Beanstalk

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Elastic Beanstalk Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, CRI Profile v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `beanstalk-enhanced-health-reporting-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die erweiterte Statusberichterstattung für Ihre AWS Elastic Beanstalk Umgebungen aktiviert ist.

Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen.

Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen. Der Elastic Beanstalk Health Agent, der in unterstützten Amazon Machine Images (AMIs) enthalten ist, wertet Protokolle und Metriken von EC2-Instances in der Umgebung aus.

Weitere Informationen finden Sie unter Verbesserte Statusberichterstattung und Überwachung im Entwicklerhandbuch.AWS Elastic Beanstalk

Abhilfe

Anweisungen zur Aktivierung der erweiterten Zustandsberichterstattung finden Sie unter Enabling enhanced Health Reporting using the Elastic Beanstalk Console im AWS Elastic Beanstalk Developer Guide.

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `elastic-beanstalk-managed-updates-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`UpdateLevel`	Stufe des Versionsupdates	Enum	`minor`, `patch`	Kein Standardwert

Dieses Steuerelement prüft, ob verwaltete Plattformupdates für eine Elastic Beanstalk Beanstalk-Umgebung aktiviert sind. Die Steuerung schlägt fehl, wenn keine Updates für verwaltete Plattformen aktiviert sind. Standardmäßig ist die Steuerung erfolgreich, wenn irgendeine Art von Plattform-Update aktiviert ist. Optional können Sie einen benutzerdefinierten Parameterwert angeben, um eine bestimmte Aktualisierungsstufe zu erfordern.

Durch die Aktivierung verwalteter Plattformupdates wird sichergestellt, dass die neuesten verfügbaren Plattformkorrekturen, Updates und Funktionen für die Umgebung installiert werden. Ein wichtiger Schritt zur Sicherung der Systeme ist es, bei der Patch-Installation auf dem Laufenden zu bleiben.

Abhilfe

Informationen zur Aktivierung verwalteter Plattformupdates finden Sie unter So konfigurieren Sie verwaltete Plattformupdates unter Verwaltete Plattformupdates im AWS Elastic Beanstalk Entwicklerhandbuch.

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

Verwandte Anforderungen: PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `elastic-beanstalk-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`RetentionInDays`	Anzahl der Tage, an denen Protokollereignisse vor Ablauf aufbewahrt werden sollen	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Kein Standardwert

Dieses Steuerelement prüft, ob eine Elastic Beanstalk Beanstalk-Umgebung so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Die Steuerung schlägt fehl, wenn eine Elastic Beanstalk Beanstalk-Umgebung nicht so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Optional können Sie einen benutzerdefinierten Wert für den `RetentionInDays` Parameter angeben, wenn Sie möchten, dass die Steuerung nur dann erfolgreich ist, wenn Logs für die angegebene Anzahl von Tagen vor Ablauf aufbewahrt werden.

CloudWatch hilft Ihnen dabei, verschiedene Messwerte für Ihre Anwendungen und Infrastrukturressourcen zu sammeln und zu überwachen. Sie können es auch verwenden CloudWatch , um Alarmaktionen auf der Grundlage bestimmter Metriken zu konfigurieren. Wir empfehlen die Integration von Elastic Beanstalk mit, CloudWatch um mehr Einblick in Ihre Elastic Beanstalk Beanstalk-Umgebung zu erhalten. Zu den Elastic Beanstalk Beanstalk-Protokollen gehören die Datei eb-activity.log, Zugriffsprotokolle vom Umgebungs-Nginx- oder Apache-Proxyserver sowie umgebungsspezifische Protokolle.

Abhilfe

Informationen zur Integration von Elastic Beanstalk mit CloudWatch Logs finden Sie im AWS Elastic Beanstalk Developer Guide unter CloudWatch Instanzprotokolle streamen.

Security Hub CSPM-Steuerelemente für Elastic Load Balancing

Diese AWS Security Hub CSPM Kontrollen bewerten den Elastic Load Balancing Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

Verwandte Anforderungen: PCI DSS v3.2. 1/23.3, PCI DSS v3.2. 1/4.1, NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: alb-http-to-https-redirection-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die HTTP-zu-HTTPS-Umleitung auf allen HTTP-Listenern von Application Load Balancers konfiguriert ist. Die Steuerung schlägt fehl, wenn für einen der HTTP-Listener von Application Load Balancers keine HTTP-zu-HTTPS-Umleitung konfiguriert ist.

Bevor Sie Ihren Application Load Balancer verwenden können, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener unterstützen sowohl das HTTP- als auch das HTTPS-Protokoll. Sie können einen HTTPS-Listener verwenden, um die Arbeit der Verschlüsselung und Entschlüsselung auf Ihren Load Balancer auszulagern. Um die Verschlüsselung während der Übertragung zu erzwingen, sollten Sie Umleitungsaktionen mit Application Load Balancers verwenden, um Client-HTTP-Anfragen an eine HTTPS-Anfrage an Port 443 umzuleiten.

Weitere Informationen finden Sie unter Listener für Ihre Application Load Balancers im Benutzerhandbuch für Application Load Balancers.

Abhilfe

Um HTTP-Anfragen an HTTPS umzuleiten, müssen Sie eine Application Load Balancer Balancer-Listener-Regel hinzufügen oder eine bestehende Regel bearbeiten.

Anweisungen zum Hinzufügen einer neuen Regel finden Sie unter Regel hinzufügen im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP und geben Sie dann ein**80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein**443**.

Anweisungen zum Bearbeiten einer vorhandenen Regel finden Sie unter Regel bearbeiten im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP und geben Sie dann ein**80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein**443**.

[ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (5) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: elb-acm-certificate-required

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Classic Load Balancer von AWS Certificate Manager (ACM) bereitgestellte HTTPS/SSL Zertifikate verwendet. Die Steuerung schlägt fehl, wenn der mit dem HTTPS/SSL Listener konfigurierte Classic Load Balancer kein von ACM bereitgestelltes Zertifikat verwendet.

Um ein Zertifikat zu erstellen, können Sie entweder ACM oder ein Tool verwenden, das die SSL- und TLS-Protokolle unterstützt, z. B. OpenSSL. Security Hub CSPM empfiehlt, dass Sie ACM verwenden, um Zertifikate für Ihren Load Balancer zu erstellen oder zu importieren.

ACM ist in Classic Load Balancers integriert, sodass Sie das Zertifikat auf Ihrem Load Balancer bereitstellen können. Sie sollten diese Zertifikate auch automatisch erneuern.

Abhilfe

Informationen zum Zuordnen eines SSL/TLS ACM-Zertifikats zu einem Classic Load Balancer finden Sie im AWS Knowledge Center-Artikel Wie kann ich ein SSL/TLS ACM-Zertifikat mit einem Classic-, Anwendungs- oder Network Load Balancer verknüpfen?

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4), NIST.800-53.r5 SC-7 (1), (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, 3.13.15, PCI DSS NIST.800-171.r2 v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: elb-tls-https-listeners-only

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer Balancer-Listener mit dem HTTPS- oder TLS-Protokoll für Front-End-Verbindungen (Client zu Load Balancer) konfiguriert sind. Die Steuerung ist anwendbar, wenn ein Classic Load Balancer über Listener verfügt. Wenn für Ihren Classic Load Balancer kein Listener konfiguriert ist, meldet die Steuerung keine Ergebnisse.

Die Steuerung ist erfolgreich, wenn die Classic Load Balancer Balancer-Listener mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert sind.

Die Steuerung schlägt fehl, wenn der Listener nicht mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert ist.

Bevor Sie mit der Verwendung eines Load Balancers beginnen, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener können sowohl HTTP als auch Protokolle unterstützen. HTTPS/TLS Sie sollten immer einen HTTPS- oder TLS-Listener verwenden, damit der Load Balancer die Ver- und Entschlüsselung während der Übertragung übernimmt.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre Listener so, dass sie das TLS- oder HTTPS-Protokoll verwenden.

Um alle nicht konformen Listener in Listener umzuwandeln TLS/HTTPS

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie Ihren Classic Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listeners die Option Edit aus.
5. Ändern Sie für alle Listener, bei denen das Load Balancer-Protokoll nicht auf HTTPS oder SSL eingestellt ist, die Einstellung auf HTTPS oder SSL.
6. Wählen Sie für alle modifizierten Listener auf der Registerkarte Zertifikate die Option Standard ändern aus.
7. Wählen Sie für ACM- und IAM-Zertifikate ein Zertifikat aus.
8. Wählen Sie Als Standard speichern aus.
9. Nachdem Sie alle Listener aktualisiert haben, wählen Sie Speichern aus.

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden

Verwandte Anforderungen: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/62.2.4, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: alb-http-drop-invalid-header-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet, ob ein Application Load Balancer so konfiguriert ist, dass er ungültige HTTP-Header löscht. Das Steuerelement schlägt fehl, wenn der Wert von auf gesetzt `routing.http.drop_invalid_header_fields.enabled` ist. `false`

Standardmäßig sind Application Load Balancer nicht so konfiguriert, dass sie ungültige HTTP-Header-Werte löschen. Durch das Entfernen dieser Header-Werte werden HTTP-Desync-Angriffe verhindert.

> **Note**
>
> Wir empfehlen, diese Steuerung zu deaktivieren, falls sie in Ihrem ELB.12 Konto aktiviert ist. Weitere Informationen finden Sie unter [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden.

Abhilfe

Um dieses Problem zu beheben, konfigurieren Sie Ihren Load Balancer so, dass ungültige Header-Felder gelöscht werden.

Um den Load Balancer so zu konfigurieren, dass ungültige Header-Felder gelöscht werden

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load balancers (Load Balancer).
3. Wählen Sie einen Application Load Balancer aus.
4. Wählen Sie unter Aktionen die Option Attribute bearbeiten aus.
5. Wählen Sie unter Ungültige Header-Felder löschen die Option Aktivieren aus.
6. Wählen Sie Speichern.

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp:`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: elb-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Application Load Balancer und der Classic Load Balancer die Protokollierung aktiviert haben. Ist dies der Fall, schlägt die Steuerung fehl. `access_logs.s3.enabled` `false`

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihren Classic Load Balancer im Benutzerhandbuch für Classic Load Balancer.

Abhilfe

Informationen zum Aktivieren von Zugriffsprotokollen finden Sie unter Schritt 3: Zugriffsprotokolle konfigurieren im Benutzerhandbuch für Application Load Balancers.

[ELB.6] Bei Anwendung, Gateway und Network Load Balancers sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: elb-deletion-protection-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Anwendung, ein Gateway oder ein Network Load Balancer der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz deaktiviert ist.

Aktivieren Sie den Löschschutz, um Ihre Anwendung, Ihr Gateway oder Ihren Network Load Balancer vor dem Löschen zu schützen.

Abhilfe

Um zu verhindern, dass der Load Balancer versehentlich gelöscht wird, können Sie den Löschschutz aktivieren. Standardmäßig ist der Löschschutz für Ihren Load Balancer deaktiviert.

Wenn Sie den Löschschutz für Ihren Load Balancer aktivieren, müssen Sie den Löschschutz deaktivieren, bevor Sie den Load Balancer löschen können.

Informationen zum Aktivieren des Löschschutzes für einen Application Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Application Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Gateway Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Gateway Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Network Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Network Load Balancer.

[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Erholung > Resilienz

Schweregrad: Niedrig

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config Regel: `elb-connection-draining-enabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei Classic Load Balancers der Verbindungsabbau aktiviert ist.

Durch die Aktivierung des Verbindungsabbaus auf Classic Load Balancers wird sichergestellt, dass der Load Balancer keine Anfragen mehr an Instances sendet, die sich abmelden oder deren

Status beeinträchtigt ist. Es hält die bestehenden Verbindungen offen. Dies ist besonders nützlich für Instances in Auto Scaling Scaling-Gruppen, um sicherzustellen, dass Verbindungen nicht abrupt unterbrochen werden.

Abhilfe

Informationen zum Aktivieren des Verbindungsabbaus auf Classic Load Balancers finden Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren im Benutzerhandbuch für Classic Load Balancers.

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: elb-predefined-security-policy-ssl-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer HTTPS/SSL Balancer-Listener die vordefinierte Richtlinie verwenden. `ELBSecurityPolicy-TLS-1-2-2017-01` Die Steuerung schlägt fehl, wenn die Classic Load Balancer HTTPS/SSL Balancer-Listener sie nicht verwenden. `ELBSecurityPolicy-TLS-1-2-2017-01`

Eine Sicherheitsrichtlinie ist eine Kombination aus SSL-Protokollen, Chiffren und der Option Server Order Preference. Vordefinierte Richtlinien steuern die Chiffren, Protokolle und Präferenzreihenfolgen, die bei SSL-Verhandlungen zwischen einem Client und einem Load Balancer unterstützt werden sollen.

Die Verwendung `ELBSecurityPolicy-TLS-1-2-2017-01` kann Ihnen dabei helfen, die Compliance- und Sicherheitsstandards zu erfüllen, nach denen Sie bestimmte Versionen von SSL und TLS deaktivieren müssen. Weitere Informationen finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancers im Benutzerhandbuch für Classic Load Balancers.

Abhilfe

Informationen zur Verwendung der vordefinierten Sicherheitsrichtlinie `ELBSecurityPolicy-TLS-1-2-2017-01` mit einem Classic Load Balancer finden Sie unter Sicherheitseinstellungen konfigurieren im Benutzerhandbuch für Classic Load Balancers.

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: elb-cross-zone-load-balancing-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der zonenübergreifende Load Balancing für die Classic Load Balancers (CLBs) aktiviert ist. Die Steuerung schlägt fehl, wenn der zonenübergreifende Lastenausgleich für einen CLB nicht aktiviert ist.

Ein Load Balancer-Knoten verteilt den Verkehr nur auf die registrierten Ziele in seiner Availability Zone. Wenn zonenübergreifendes Load Balancing deaktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig nur auf die registrierten Ziele in seiner Availability Zone. Wenn die Anzahl der registrierten Ziele in den Availability Zones nicht identisch ist, wird der Verkehr nicht gleichmäßig verteilt und die Instances in einer Zone werden möglicherweise im Vergleich zu den Instances in einer anderen Zone überlastet. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten für Ihren Classic Load Balancer Anfragen gleichmäßig auf die registrierten Instances in allen aktivierten Availability Zones. Einzelheiten finden Sie unter Cross-zone Load Balancing im Elastic Load Balancing User Guide.

Abhilfe

Informationen zur Aktivierung von zonenübergreifendem Load Balancing in einem Classic Load Balancer finden Sie unter Aktivieren von zonenübergreifendem Load Balancing im Benutzerhandbuch für Classic Load Balancer.

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: clb-multiple-az

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob ein Classic Load Balancer so konfiguriert wurde, dass er sich über mindestens die angegebene Anzahl von Availability Zones (AZs) erstreckt. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mindestens die angegebene Anzahl von AZs umfasst. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub CSPM einen Standardwert von zwei AZs.

Ein Classic Load Balancer kann so eingerichtet werden, dass eingehende Anfragen auf Amazon EC2 EC2-Instances in einer einzigen Availability Zone oder mehreren Availability Zones verteilt werden. Ein Classic Load Balancer, der sich nicht über mehrere Availability Zones erstreckt, kann den Traffic nicht zu Zielen in einer anderen Availability Zone umleiten, wenn die einzige konfigurierte Availability Zone nicht mehr verfügbar ist.

Abhilfe

Informationen zum Hinzufügen von Availability Zones zu einem Classic Load Balancer finden Sie unter Hinzufügen oder Entfernen von Subnetzen für Ihren Classic Load Balancer im Benutzerhandbuch für Classic Load Balancer.

[ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), PCI DSS v4.0. NIST.800-53.r5 CM-2 1/62.2.4, CRI-Profil v2. 2/GV. OC-04.03, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Schützen > Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: alb-desync-mode-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `desyncMode`: `defensive, strictest` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Application Load Balancer mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist. Die Steuerung schlägt fehl, wenn ein Application Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum dazu führen, dass Anmeldeinformationen überlastet

werden oder nicht autorisierte Befehle ausgeführt werden. Application Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Minimierungsmodus eines Application Load Balancer finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

[ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: elbv2-multiple-az

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	2

Dieses Steuerelement prüft, ob ein Elastic Load Balancer V2 (Application, Network oder Gateway Load Balancer) Instances aus mindestens der angegebenen Anzahl von Availability Zones (AZs)

registriert hat. Die Kontrolle schlägt fehl, wenn bei einem Elastic Load Balancer V2 keine Instances in mindestens der angegebenen Anzahl von AZs registriert sind. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub CSPM einen Standardwert von zwei AZs.

Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. EC2-Instances, Container und IP-Adressen oder eine oder mehrere Availability Zones. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es wird empfohlen, mindestens zwei Availability Zones zu konfigurieren, um die Verfügbarkeit von Diensten sicherzustellen, da der Elastic Load Balancer den Traffic in eine andere Availability Zone weiterleiten kann, falls eine nicht verfügbar ist. Durch die Konfiguration mehrerer Availability Zones wird vermieden, dass es für die Anwendung nur einen einzigen Fehlerpunkt gibt.

Abhilfe

Informationen zum Hinzufügen einer Availability Zone zu einem Application Load Balancer finden Sie unter Availability Zones for your Application Load Balancer im Benutzerhandbuch für Application Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Network Load Balancer finden Sie unter Network Load Balancers im Benutzerhandbuch für Network Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Gateway Load Balancer finden Sie unter Erstellen eines Gateway Load Balancers im Benutzerhandbuch für Gateway Load Balancer.

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), PCI DSS v4.0. NIST.800-53.r5 CM-2 1/62.2.4, CRI-Profil v2. 2/GV. OC-04.03, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Schützen > Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: clb-desync-mode-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `desyncMode`: `defensive, strictest` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Classic Load Balancer mit einem defensiven oder dem strengsten Desync-Minimierungsmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum zum Entführen von Anmeldeinformationen oder zur Ausführung nicht autorisierter Befehle führen. Classic Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Mitigationsmodus auf einem Classic Load Balancer finden Sie unter Ändern des Desync-Mitigationsmodus im Benutzerhandbuch für Classic Load Balancer.

[ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: alb-waf-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Application Load Balancer einer AWS WAF Classic- oder AWS WAF Web-Zugriffskontrollliste (Web-ACL) zugeordnet ist. Die Steuerung schlägt fehl, wenn das `Enabled` Feld für die AWS WAF Konfiguration auf `false` gesetzt ist.

AWS WAF ist eine Firewall für Webanwendungen, die hilft, Webanwendungen und APIs vor Angriffen zu schützen. Mit AWS WAF können Sie eine Web-ACL konfigurieren, bei der es sich um eine Reihe

von Regeln handelt, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Wir empfehlen, Ihren Application Load Balancer mit einer AWS WAF Web-ACL zu verknüpfen, um ihn vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Zuordnen eines Application Load Balancer zu einer Web-ACL finden Sie unter Web-ACL mit einer AWS Ressource verknüpfen oder deren Zuordnung aufheben im Developer Guide.AWS WAF

[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config -Regel: elbv2-predefined-security-policy-ssl-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:`sslPolicies`: `ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-PQ-2025-09, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09` (nicht anpassbar)

Dieses Steuerelement prüft, ob der HTTPS-Listener für einen Application Load Balancer oder der TLS-Listener für einen Network Load Balancer so konfiguriert ist, dass Daten während der Übertragung mithilfe einer empfohlenen Sicherheitsrichtlinie verschlüsselt werden. Die Steuerung schlägt fehl, wenn der HTTPS- oder TLS-Listener für einen Load Balancer nicht für die Verwendung einer empfohlenen Sicherheitsrichtlinie konfiguriert ist.

Elastic Load Balancing verwendet eine SSL-Verhandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um Verbindungen zwischen einem Client und einem Load Balancer auszuhandeln. Die Sicherheitsrichtlinie spezifiziert eine Kombination von Protokollen und Chiffren. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her. Eine Chiffre ist ein Verschlüsselungsalgorithmus, der Verschlüsselungsschlüssel verwendet, um eine codierte Nachricht zu erstellen. Während der Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Die Verwendung einer empfohlenen Sicherheitsrichtlinie für einen Load Balancer kann Ihnen helfen, die Compliance- und Sicherheitsstandards einzuhalten.

Abhilfe

Informationen zu empfohlenen Sicherheitsrichtlinien und zur Aktualisierung von Listenern finden Sie in den folgenden Abschnitten der Elastic Load Balancing Balancing-Benutzerhandbücher: Sicherheitsrichtlinien für Application Load Balancer, Sicherheitsrichtlinien für Network Load Balancer, Aktualisieren eines HTTPS-Listeners für Ihren Application Load Balancer und Aktualisieren eines Listeners für Ihren Network Load Balancer.

[ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config -Regel: elbv2-listener-encryption-in-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Listener für einen Application Load Balancer oder Network Load Balancer so konfiguriert ist, dass er ein sicheres Protokoll für die Verschlüsselung von Daten während der Übertragung verwendet. Die Steuerung schlägt fehl, wenn ein Application Load Balancer Balancer-Listener nicht für die Verwendung des HTTPS-Protokolls konfiguriert ist oder ein Network Load Balancer Balancer-Listener nicht für die Verwendung des TLS-Protokolls konfiguriert ist.

Um Daten zu verschlüsseln, die zwischen einem Client und einem Load Balancer übertragen werden, sollten die Elastic Load Balancer Balancer-Listener so konfiguriert werden, dass sie branchenübliche Sicherheitsprotokolle verwenden: HTTPS für Application Load Balancers oder TLS für Network Load Balancers. Andernfalls sind Daten, die zwischen einem Client und einem Load Balancer übertragen werden, anfällig für Abfangen, Manipulation und unbefugten Zugriff. Die Verwendung von HTTPS oder TLS durch einen Zuhörer entspricht den bewährten Sicherheitsverfahren und trägt dazu bei, die Vertraulichkeit und Integrität der Daten während der Übertragung zu gewährleisten. Dies ist besonders wichtig für Anwendungen, die vertrauliche Informationen verarbeiten oder Sicherheitsstandards einhalten müssen, die eine Verschlüsselung von Daten bei der Übertragung erfordern.

Abhilfe

Informationen zur Konfiguration von Sicherheitsprotokollen für Listener finden Sie in den folgenden Abschnitten der Elastic Load Balancing Balancing-Benutzerhandbücher: Einen HTTPS-Listener für Ihren Application Load Balancer erstellen und Einen Listener für Ihren Network Load Balancer erstellen.

[ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config -Regel: elbv2-targetgroup-healthcheck-protocol-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft, ob die Zielgruppe für Integritätsprüfungen von Anwendungen und Network Load Balancer ein verschlüsseltes Transportprotokoll verwendet. Die Steuerung schlägt fehl, wenn das Protokoll zur Integritätsprüfung kein HTTPS verwendet. Dieses Steuerelement gilt nicht für Lambda-Zieltypen.

Load Balancer senden Anfragen zur Integritätsprüfung an registrierte Ziele, um deren Status zu ermitteln und den Verkehr entsprechend weiterzuleiten. Das in der Zielgruppenkonfiguration

angegebene Protokoll zur Integritätsprüfung bestimmt, wie diese Prüfungen durchgeführt werden. Wenn Integritätsprüfungsprotokolle unverschlüsselte Kommunikation wie HTTP verwenden, können die Anfragen und Antworten während der Übertragung abgefangen oder manipuliert werden. Auf diese Weise können Angreifer Einblicke in die Infrastrukturkonfiguration gewinnen, die Ergebnisse von Integritätsprüfungen manipulieren oder Man-in-the-Middle-Angriffe durchführen, die sich auf Routing-Entscheidungen auswirken. Die Verwendung von HTTPS für Integritätsprüfungen ermöglicht eine verschlüsselte Kommunikation zwischen dem Load Balancer und seinen Zielen und schützt so die Integrität und Vertraulichkeit der Gesundheitsstatusinformationen.

Abhilfe

Informationen zur Konfiguration verschlüsselter Zustandsprüfungen für Ihre Application Load Balancer Balancer-Zielgruppe finden Sie unter Aktualisieren der Health Check-Einstellungen einer Application Load Balancer Balancer-Zielgruppe im Elastic Load Balancing Balancer-Benutzerhandbuch. Informationen zur Konfiguration verschlüsselter Zustandsprüfungen für Ihre Network Load Balancer Balancer-Zielgruppe finden Sie unter Aktualisieren der Einstellungen für die Zustandsprüfung einer Network Load Balancer Balancer-Zielgruppe im Elastic Load Balancing Balancer-Benutzerhandbuch.

[ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config -Regel: elbv2-targetgroup-protocol-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Elastic Load Balancing Balancing-Zielgruppe ein verschlüsseltes Transportprotokoll verwendet. Diese Kontrolle gilt nicht für Zielgruppen mit einem Zieltyp von Lambda oder ALB oder Zielgruppen, die das GENEVE-Protokoll verwenden. Die Kontrolle schlägt fehl, wenn die Zielgruppe kein HTTPS-, TLS- oder QUIC-Protokoll verwendet.

Die Verschlüsselung von Daten während der Übertragung schützt sie vor dem Abfangen durch unbefugte Benutzer. Zielgruppen, die unverschlüsselte Protokolle (HTTP, TCP, UDP) verwenden,

übertragen Daten unverschlüsselt und sind somit anfällig für Abhörversuche. Durch die Verwendung verschlüsselter Protokolle (HTTPS, TLS, QUIC) wird sichergestellt, dass die zwischen Load Balancern und Zielen übertragenen Daten geschützt sind.

Abhilfe

Um ein verschlüsseltes Protokoll zu verwenden, müssen Sie eine neue Zielgruppe mit dem HTTPS-, TLS- oder QUIC-Protokoll erstellen. Das Zielgruppenprotokoll kann nach der Erstellung nicht geändert werden. Informationen zur Erstellung einer Application Load Balancer-Zielgruppe finden Sie unter Erstellen einer Zielgruppe für Ihren Application Load Balancer im Elastic Load Balancing Balancing-Benutzerhandbuch. Informationen zur Erstellung einer Network Load Balancer-Zielgruppe finden Sie unter Erstellen einer Zielgruppe für Ihren Network Load Balancer im Elastic Load Balancing Balancing-Benutzerhandbuch.

Security Hub CSPM für Elasticsearch

Diese AWS Security Hub CSPM Kontrollen bewerten den Elasticsearch-Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2. 1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-encrypted-at-rest`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten sollten Sie Ihre Daten so konfigurieren OpenSearch, OpenSearch dass sie im Ruhezustand verschlüsselt werden. Elasticsearch-Domains bieten die Verschlüsselung von Daten im Ruhezustand. Die Funktion dient AWS KMS zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel. Für die Verschlüsselung wird der Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln () AES-256 verwendet.

Weitere Informationen zur OpenSearch Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

Bestimmte Instance-Typen, wie z. B. `t.small` und`t.medium`, unterstützen die Verschlüsselung von Daten im Ruhezustand nicht. Einzelheiten finden Sie unter Unterstützte Instance-Typen im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende Elasticsearch-Domains finden Sie unter Enabling encryption of data at rest im Amazon OpenSearch Service Developer Guide.

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-in-vpc-only`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Weitere Resource-basedInformationen finden Sie im Amazon OpenSearch Service Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. Bewährte Sicherheitsmethoden für Ihre VPC finden Sie im Amazon VPC-Benutzerhandbuch.

Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkkontrollen, um den Zugriff auf Elasticsearch-Domains zu sichern, darunter Netzwerk-ACL und Sicherheitsgruppen. Security Hub CSPM empfiehlt, öffentliche Elasticsearch-Domains zu VPCs zu migrieren, um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder eine andere Domäne erstellen oder dieses Steuerelement deaktivieren.

Weitere Informationen finden Sie unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC im Amazon OpenSearch Service Developer Guide.

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4,, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-node-to-node-encryption-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Elasticsearch-Domain die Verschlüsselung von Knoten zu Knoten aktiviert ist. Die Kontrolle schlägt fehl, wenn für die Elasticsearch-Domain die Verschlüsselung von Knoten zu Knoten nicht aktiviert ist. Das Steuerelement führt auch zu fehlgeschlagenen Ergebnissen, wenn eine Elasticsearch-Version keine Verschlüsselungsprüfungen von Knoten zu Knoten unterstützt.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit Person-in-the-Middle- oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der Knoten-zu-Knoten-Verschlüsselung für Elasticsearch-Domains wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zur Aktivierung der Knoten-zu-Knoten-Verschlüsselung für neue und bestehende Domains finden Sie unter Enabling Node-to-Knoten-Verschlüsselung im Amazon Service Developer Guide. OpenSearch

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren - Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `logtype = 'error'`(nicht anpassbar)

Dieses Steuerelement prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden.

Sie sollten Fehlerprotokolle für Elasticsearch-Domains aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Beantwortung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zur Aktivierung der Protokollveröffentlichung finden Sie unter Aktivieren der Protokollveröffentlichung (Konsole) im Amazon OpenSearch Service Developer Guide.

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-audit-logging-enabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar). Security Hub CSPM füllt diesen Parameter nicht aus. Comma-separated Liste der CloudWatch Log-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

  Diese Regel gilt, `NON_COMPLIANT` wenn die CloudWatch Logs-Log-Gruppe der Elasticsearch-Domain in dieser Parameterliste nicht angegeben ist.

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Audit-Protokollierung aktiviert ist. Diese Kontrolle schlägt fehl, wenn für eine Elasticsearch-Domain die Audit-Protokollierung nicht aktiviert ist.

Audit-Logs sind hochgradig anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren Elasticsearch-Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Detaillierte Anweisungen zur Aktivierung von Audit-Logs finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service Developer Guide.

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-data-node-fault-tolerance` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist`true`.

Eine Elasticsearch-Domain benötigt aus Gründen der Hochverfügbarkeit und Fehlertoleranz mindestens drei Datenknoten. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei Datenknoten gewährleistet den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer Elasticsearch-Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.

2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl ein, die größer oder gleich ist3.

   Legen Sie für Bereitstellungen mit drei Availability Zones den Wert auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.
5. Wählen Sie Absenden aus.

[ES.7] Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-primary-node-fault-tolerance` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei dedizierten Primärknoten konfiguriert sind. Diese Kontrolle schlägt fehl, wenn die Domain keine dedizierten Primärknoten verwendet. Diese Kontrolle gilt als bestanden, wenn Elasticsearch-Domänen über fünf dedizierte Primärknoten verfügen. Die Verwendung von mehr als drei Primärknoten ist jedoch möglicherweise unnötig, um das Verfügbarkeitsrisiko zu minimieren, und führt zu zusätzlichen Kosten.

Für eine Elasticsearch-Domain sind mindestens drei dedizierte Primärknoten erforderlich, um eine hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten. Dedizierte Primärknotenressourcen können bei der blue/green Bereitstellung von Datenknoten belastet werden, da zusätzliche Knoten verwaltet werden müssen. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei dedizierten

Primärknoten gewährleistet eine ausreichende Ressourcenkapazität des Primärknotens und den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der dedizierten Primärknoten in einer OpenSearch Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.
2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Dedizierte Masterknoten den Instanztyp auf den gewünschten Instanztyp ein.
5. Stellen Sie die Anzahl der Master-Knoten auf drei oder mehr ein.
6. Wählen Sie Absenden aus.

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-https-required` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dadurch wird geprüft, ob ein Elasticsearch-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Steuerung schlägt fehl, wenn der Elasticsearch-Domänenendpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert

ist oder wenn HTTPS nicht aktiviert ist. Die aktuell neueste unterstützte TLS-Sicherheitsrichtlinie ist`Policy-Min-TLS-1-2-PFS-2023-10`.

HTTPS (TLS) kann verwendet werden, um potenzielle Angreifer daran zu hindern, Person-in-the-Middle- oder ähnliche Angriffe zu nutzen, um den Netzwerkverkehr abzuhören oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Um die TLS-Verschlüsselung zu aktivieren, verwenden Sie den UpdateDomainConfigAPI-Vorgang, um das DomainEndpointOptionsObjekt zu konfigurieren. Dies legt die fest`TLSSecurityPolicy`.

[ES.9] Elasticsearch-Domains sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `tagged-elasticsearch-domain` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine Elasticsearch-Domain Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Elasticsearch-Domain finden Sie unter Arbeiten mit Tags im Amazon OpenSearch Service Developer Guide.

Security Hub CSPM-Steuerelemente für Amazon EMR

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon EMR (früher Amazon Elastic genannt MapReduce). Die Kontrollen sind möglicherweise nicht in allen

AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EMR::Cluster`

AWS Config Regel: emr-master-no-public-ip

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Master-Knoten auf Amazon EMR-Clustern öffentliche IP-Adressen haben. Die Kontrolle schlägt fehl, wenn öffentliche IP-Adressen einer der Master-Node-Instances zugeordnet sind.

Öffentliche IP-Adressen werden im `PublicIp` Feld der `NetworkInterfaces` Konfiguration für die Instanz angegeben. Dieses Steuerelement überprüft nur Amazon EMR-Cluster, die sich im `WAITING` Status `RUNNING` oder befinden.

Abhilfe

Während des Starts können Sie steuern, ob Ihrer Instance in einem Standard- oder einem anderen Subnetz eine öffentliche IPv4-Adresse zugewiesen wird. In Standard-Subnetzen ist dieses Attribut standardmäßig auf gesetzt. `true` Bei nicht standardmäßigen Subnetzen ist das IPv4-Attribut für öffentliche Adressierung auf gesetzt`false`, sofern es nicht vom Amazon EC2 EC2-Instance-Startassistenten erstellt wurde. In diesem Fall ist das Attribut auf gesetzt. `true`

Nach dem Start können Sie eine öffentliche IPv4-Adresse nicht manuell von Ihrer Instance trennen.

Um ein fehlgeschlagenes Ergebnis zu beheben, müssen Sie einen neuen Cluster in einer VPC mit einem privaten Subnetz starten, für das das IPv4-Attribut für öffentliche Adressierung auf gesetzt ist. `false` Anweisungen finden Sie unter Cluster in einer VPC starten im Amazon EMR Management Guide.

[EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config Regel: emr-block-public-access

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Ihr Konto mit Amazon EMR konfiguriert ist, um den öffentlichen Zugriff zu blockieren. Die Kontrolle schlägt fehl, wenn die Einstellung „Öffentlichen Zugriff blockieren“ nicht aktiviert ist oder wenn ein anderer Port als Port 22 zulässig ist.

Amazon EMR Block Public Access verhindert, dass Sie einen Cluster in einem öffentlichen Subnetz starten, wenn der Cluster über eine Sicherheitskonfiguration verfügt, die eingehenden Datenverkehr von öffentlichen IP-Adressen an einem Port zulässt. Wenn ein Benutzer von Ihrem AWS-Konto einen Cluster startet, überprüft Amazon EMR die Portregeln in der Sicherheitsgruppe für den Cluster und vergleicht sie mit Ihren Regeln für eingehenden Datenverkehr. Wenn die Sicherheitsgruppe über eine Regel für eingehenden Datenverkehr verfügt, die Ports zu den öffentlichen IP-Adressen öffnet, IPv4 0.0.0. 0/0 oder IPv6: :/0, und diese Ports sind nicht als Ausnahmen für Ihr Konto angegeben, Amazon EMR lässt den Benutzer den Cluster nicht erstellen.

> **Note**
>
> Den öffentlichen Zugriff blockieren ist standardmäßig aktiviert. Um den Kontoschutz zu erhöhen, empfehlen wir, ihn aktiviert zu lassen.

Abhilfe

Informationen zur Konfiguration von Block Public Access für Amazon EMR finden Sie unter Using Amazon EMR block public access im Amazon EMR Management Guide.

[EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8) NIST.800-53.r5 SI-12, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::EMR::SecurityConfiguration`

AWS Config -Regel: emr-security-configuration-encryption-rest

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon EMR-Sicherheitskonfiguration die Verschlüsselung im Ruhezustand aktiviert ist. Die Kontrolle schlägt fehl, wenn die Sicherheitskonfiguration die Verschlüsselung im Ruhezustand nicht aktiviert.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand in einer Amazon EMR-Sicherheitskonfiguration finden Sie unter Datenverschlüsselung konfigurieren im Amazon EMR Management Guide.

[EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::EMR::SecurityConfiguration`

AWS Config -Regel: emr-security-configuration-encryption-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob in einer Amazon EMR-Sicherheitskonfiguration die Verschlüsselung bei der Übertragung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Sicherheitskonfiguration die Verschlüsselung bei der Übertragung nicht aktiviert.

Daten bei der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein unbefugter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung bei der Übertragung in einer Amazon EMR-Sicherheitskonfiguration finden Sie unter Datenverschlüsselung konfigurieren im Amazon EMR Management Guide.

Security Hub CSPM-Steuerungen für EventBridge

Diese AWS Security Hub CSPM Kontrollen bewerten den EventBridge Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EventBridge.2] EventBridge Eventbusse sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Events::EventBus`

AWS Config Regel: `tagged-events-eventbus` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EventBridge Amazon-Event-Bus Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Event-Bus keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Event-Bus mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie

außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EventBridge Event-Bus finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/103.3.1, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Niedrig

Art der Ressource: `AWS::Events::EventBus`

AWS Config -Regel: custom-eventbus-policy-attached

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein EventBridge benutzerdefinierter Amazon Event Bus mit einer ressourcenbasierten Richtlinie verknüpft ist. Diese Steuerung schlägt fehl, wenn dem benutzerdefinierten Event-Bus keine ressourcenbasierte Richtlinie zugewiesen wurde.

Standardmäßig ist an einen EventBridge benutzerdefinierten Ereignisbus keine ressourcenbasierte Richtlinie angehängt. Dadurch können die Principals im Konto auf den Event-Bus zugreifen. Indem Sie eine ressourcenbasierte Richtlinie an den Event-Bus anhängen, können Sie den Zugriff auf den Event-Bus auf bestimmte Konten beschränken und Entitäten in einem anderen Konto bewusst Zugriff gewähren.

Abhilfe

Informationen zum Anhängen einer ressourcenbasierten Richtlinie an einen EventBridge benutzerdefinierten Event-Bus finden Sie unter Using Resource Based Policies for Amazon EventBridge im Amazon-Benutzerhandbuch. EventBridge

[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Events::Endpoint`

AWS Config -Regel: `global-endpoint-event-replication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Ereignisreplikation für einen EventBridge globalen Amazon-Endpunkt aktiviert ist. Die Steuerung schlägt fehl, wenn die Ereignisreplikation für einen globalen Endpunkt nicht aktiviert ist.

Globale Endpunkte tragen dazu bei, dass Ihre Anwendung Regional-fault tolerant wird. Zunächst weisen Sie dem Endpunkt eine Amazon-Route-53-Zustandsprüfung zu. Wenn ein Failover initiiert wird, meldet die Integritätsprüfung einen „fehlerhaften“ Zustand. Innerhalb weniger Minuten nach

der Einleitung des Failovers werden alle benutzerdefinierten Ereignisse an einen Event Bus in der sekundären Region weitergeleitet und von diesem Event Bus verarbeitet. Wenn Sie globale Endpunkte verwenden, können Sie die Ereignisreplikation aktivieren. Bei der Ereignisreplikation werden alle benutzerdefinierten Ereignisse mithilfe verwalteter Regeln an die Event Buses in der primären und sekundären Region gesendet. Wir empfehlen, die Ereignisreplikation bei der Einrichtung globaler Endgeräte zu aktivieren. Mithilfe der Ereignisreplikation können Sie überprüfen, ob Ihre globalen Endpunkte korrekt konfiguriert sind. Für die automatische Wiederherstellung nach einem Failover-Ereignis ist die Ereignisreplikation erforderlich. Wenn Sie die Ereignisreplikation nicht aktiviert haben, müssen Sie die Route 53-Zustandsprüfung manuell auf „Fehlerfrei“ zurücksetzen, bevor Ereignisse zurück in die primäre Region umgeleitet werden.

> **Note**
>
> Wenn Sie benutzerdefinierte Ereignisbusse verwenden, benötigen Sie in jeder Region einen benutzerdefinierten geraden Bus mit demselben Namen und demselben Konto, damit der Failover ordnungsgemäß funktioniert. Wenn Sie die Ereignisreplikation aktivieren, können sich Ihre monatlichen Kosten erhöhen. Informationen zu den Preisen finden Sie unter EventBridge Amazon-Preise.

Abhilfe

Informationen zum Aktivieren der Ereignisreplikation für EventBridge globale Endgeräte finden Sie unter Erstellen eines globalen Endpunkts im EventBridge Amazon-Benutzerhandbuch. Wählen Sie für die Ereignisreplikation die Option Ereignisreplikation aktiviert aus.

Security Hub CSPM-Steuerungen für Amazon Fraud Detector

Diese Security Hub CSPM-Kontrollen bewerten den Service und die Ressourcen von Amazon Fraud Detector.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::EntityType`

AWS Config-Regel: `frauddetector-entity-type-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Entitätstyp von Amazon Fraud Detector Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Die Kontrolle schlägt fehl, wenn der Entitätstyp keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Entitätstyp mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Amazon Fraud Detector Detector-Entitätstyp hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter https://console.aws.amazon.com/frauddetector.
2. Wählen Sie im Navigationsbereich Entitäten aus.
3. Wählen Sie einen Entitätstyp aus der Liste aus.
4. Wählen Sie im Abschnitt Entitätstyp-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::Label`

AWS Config-Regel: `frauddetector-label-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob ein Amazon Fraud Detector-Label Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Kontrolle schlägt fehl, wenn das Etikett keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Label mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Amazon Fraud Detector-Label hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter https://console.aws.amazon.com/frauddetector.
2. Wählen Sie im Navigationsbereich Labels aus.
3. Wählen Sie ein Etikett aus der Liste aus.
4. Wählen Sie im Bereich Label-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::Outcome`

AWS Config-Regel: `frauddetector-outcome-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob ein Ergebnis von Amazon Fraud Detector Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Kontrolle schlägt fehl, wenn das Ergebnis keine Tag-Schlüssel enthält oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Ergebnis mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Ergebnis von Amazon Fraud Detector hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter https://console.aws.amazon.com/frauddetector.
2. Wählen Sie im Navigationsbereich Outcomes aus.
3. Wählen Sie ein Ergebnis aus der Liste aus.
4. Wählen Sie im Abschnitt Ergebnis-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::Variable`

AWS Config-Regel: `frauddetector-variable-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Fraud Detector Detector-Variable Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn die Variable keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Variable mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einer Amazon Fraud Detector Detector-Variablen hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter https://console.aws.amazon.com/frauddetector.
2. Wählen Sie im Navigationsbereich Variablen aus.
3. Wählen Sie eine Variable aus der Liste aus.
4. Wählen Sie im Bereich Variablen-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

Security Hub CSPM-Steuerungen für Amazon FSx

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon FSx. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2, CRI Profile v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-07.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: fsx-openzfs-copy-tags-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon FSx for OpenZFS-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das OpenZFS-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines FSx for OpenZFS-Dateisystems zum Kopieren von Tags auf Backups und Volumes finden Sie unter Aktualisieren eines Dateisystems im Amazon FSX for OpenZFS-Benutzerhandbuch.

[FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

Verwandte Anforderungen: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8, CRI Profile v2. 2/ID. AM-02.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: fsx-lustre-copy-tags-to-backups

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon FSx for Lustre-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das Lustre-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines FSx for Lustre-Dateisystems zum Kopieren von Tags in Backups finden Sie unter Kopieren von Backups innerhalb derselben AWS-Konto im Amazon FSx for Lustre-Benutzerhandbuch.

[FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ

Verwandte Anforderungen: CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: fsx-openzfs-deployment-type-check

Art des Zeitplans: Periodisch

Parameter: `deploymentTypes: MULTI_AZ_1` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Amazon FSx for OpenZFS-Dateisystem für die Verwendung des Bereitstellungstyps Multiple Availability Zones (Multi-AZ) konfiguriert ist. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung des Bereitstellungstyps konfiguriert ist. Multi-AZ

Amazon FSx for OpenZFS unterstützt verschiedene Bereitstellungstypen für Dateisysteme: Multi-AZ (HA), Single-AZ (HA) und Single-AZ (nicht HA). Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Multi-AZ (HA) -Dateisysteme bestehen aus zwei Dateiservern mit hoher Verfügbarkeit (HA), die auf zwei Availability Zones (AZs) verteilt sind. Wir empfehlen, den Bereitstellungstyp Multi-AZ (HA) für die meisten Produktionsworkloads zu verwenden, da er ein Modell mit hoher Verfügbarkeit und Beständigkeit bietet.

Abhilfe

Sie können ein Amazon FSx for OpenZFS-Dateisystem so konfigurieren, dass es den Multi-AZ Bereitstellungstyp verwendet, wenn Sie das Dateisystem erstellen. Sie können den Bereitstellungstyp für ein vorhandenes FSx for OpenZFS-Dateisystem nicht ändern.

Informationen zu Bereitstellungstypen und Optionen für FSx für OpenZFS-Dateisysteme finden Sie unter Verfügbarkeit und Haltbarkeit für Amazon FSx für OpenZFS und Verwaltung von Dateisystemressourcen im Amazon FSx for OpenZFS-Benutzerhandbuch.

[FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: fsx-ontap-deployment-type-check

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`deploymentTypes`	Eine Liste der Bereitstellungstypen, die in die Bewertung einbezogen werden sollen. Das Steuerelement generiert einen `FAILED` Befund, wenn ein Dateisystem nicht für die Verwendung eines in der Liste angegebenen Bereitstellungstyps konfiguriert ist.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Dieses Steuerelement prüft, ob ein Amazon FSx for NetApp ONTAP-Dateisystem für die Verwendung eines Bereitstellungstyps mit mehreren Availability Zones (Multi-AZ) konfiguriert ist. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung eines Multi-AZ Bereitstellungstyps konfiguriert ist. Sie können optional eine Liste von Bereitstellungstypen angeben, die in die Bewertung einbezogen werden sollen.

Amazon FSx for NetApp ONTAP unterstützt mehrere Bereitstellungstypen für Dateisysteme: Single-AZ 1, Single-AZ 2, Multi-AZ 1 und Multi-AZ 2. Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Aufgrund des hohen Verfügbarkeits- und Dauerhaftigkeitsmodells, das diese Multi-AZ Bereitstellungstypen bieten, empfehlen wir, für die meisten Produktionsworkloads einen Multi-AZ Bereitstellungstyp zu verwenden. Multi-AZ Dateisysteme unterstützen alle Verfügbarkeits- und Haltbarkeitsfunktionen von Single-AZ Dateisystemen. Darüber hinaus sind sie so konzipiert, dass Daten auch dann kontinuierlich verfügbar sind, wenn eine Availability Zone (AZ) nicht verfügbar ist.

Abhilfe

Sie können den Bereitstellungstyp für ein vorhandenes Amazon FSx for NetApp ONTAP-Dateisystem nicht ändern. Sie können die Daten jedoch sichern und sie dann auf einem neuen Dateisystem wiederherstellen, das einen Multi-AZ Bereitstellungstyp verwendet.

Informationen zu Bereitstellungstypen und Optionen für FSx für ONTAP-Dateisysteme finden Sie unter Verfügbarkeit, Haltbarkeit und Bereitstellungsoptionen und Verwaltung von Dateisystemen im FSx for ONTAP-Benutzerhandbuch.

[FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein

Verwandte Anforderungen: CRI Profile v2. 2/GV. OC-04.03, CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: fsx-windows-deployment-type-check

Art des Zeitplans: Periodisch

Parameter: `deploymentTypes: MULTI_AZ_1` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Dateisystem von Amazon FSx for Windows File Server so konfiguriert ist, dass es den Bereitstellungstyp Multiple Availability Zones (Multi-AZ) verwendet. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung des Multi-AZ Bereitstellungstyps konfiguriert ist.

Amazon FSx for Windows File Server unterstützt zwei Bereitstellungstypen für Dateisysteme: Single-AZund Multi-AZ. Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Single-AZ Dateisysteme bestehen aus einer einzelnen Windows-Dateiserverinstanz und einer Reihe von Speichervolumes innerhalb einer einzigen Availability Zone (AZ). Multi-AZ Dateisysteme bestehen aus einem Hochverfügbarkeitscluster von Windows-Dateiservern, die auf zwei Availability Zones verteilt sind. Wir empfehlen, den Multi-AZ Bereitstellungstyp für die meisten Produktionsworkloads zu verwenden, da er ein Modell mit hoher Verfügbarkeit und Beständigkeit bietet.

Abhilfe

Sie können ein Dateisystem von Amazon FSx für Windows so konfigurieren, dass es den Multi-AZ Bereitstellungstyp verwendet, wenn Sie das Dateisystem erstellen. Sie können den Bereitstellungstyp für ein vorhandenes Dateisystem FSx for Windows File Server nicht ändern.

Informationen zu Bereitstellungstypen und Optionen für FSx für Windows File Server-Dateisysteme finden Sie unter Verfügbarkeit und Haltbarkeit: Single-AZ und Multi-AZ Dateisysteme und Erste Schritte mit Amazon FSx for Windows File Server im Amazon FSx for Windows File Server Server-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Global Accelerator

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Global Accelerator Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbarAWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GlobalAccelerator::Accelerator`

AWS ConfigRegel: `tagged-globalaccelerator-accelerator` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS Global Accelerator Accelerator über Tags mit den spezifischen Tasten verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Beschleuniger keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Beschleuniger mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Global Accelerator Global Accelerator finden Sie unter Tagging in AWS Global Accelerator im AWS Global Accelerator Developer Guide.

Security Hub CSPM-Steuerungen für AWS Glue

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Glue Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Glue.1] AWS Glue Jobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Glue::Job`

AWS Config Regel: `tagged-glue-job` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Glue Job über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Job keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Job mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einem AWS Glue Job finden Sie unter AWS Stichwörter AWS Glue im AWS Glue Benutzerhandbuch.

[Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::Glue::MLTransform`

AWS Config -Regel: glue-ml-transform-encrypted-at-rest

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Nein

Dieses Steuerelement prüft, ob eine Transformation für AWS Glue maschinelles Lernen im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Transformation für maschinelles Lernen im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung für AWS Glue Machine-Learning-Transformationen finden Sie unter Arbeiten mit Transformationen für maschinelles Lernen im AWS Glue Benutzerhandbuch.

[Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), CRI Profile v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::Glue::Job`

AWS Config -Regel: glue-spark-job-supported-version

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:`minimumSupportedGlueVersion`: `3.0` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein AWS Glue for Spark-Job so konfiguriert ist, dass er auf einer unterstützten Version von ausgeführt wird AWS Glue. Das Steuerelement schlägt fehl, wenn der Spark-Job so konfiguriert ist AWS Glue , dass er auf einer älteren Version als der unterstützten Mindestversion ausgeführt wird.

> **Note**
>
> Dieses Steuerelement generiert auch einen `FAILED` Befund AWS Glue für einen Spark-Job, wenn die Eigenschaft AWS Glue version (`GlueVersion`) nicht existiert oder im Configuration Item (CI) für den Job Null ist. In solchen Fällen enthält das Ergebnis die folgende Anmerkung:`GlueVersion is null or missing in glueetl job configuration`. Um diese Art von `FAILED` Befund zu beheben, fügen Sie die `GlueVersion` Eigenschaft der Konfiguration des Jobs hinzu. Eine Liste der unterstützten Versionen und Laufzeitumgebungen finden Sie im AWS Glue Benutzerhandbuch unter AWS Glue Versionen.

Das Ausführen von AWS Glue Spark-Jobs auf aktuellen Versionen von AWS Glue kann die Leistung, Sicherheit und den Zugriff auf die neuesten Funktionen von optimieren AWS Glue. Es kann auch zum Schutz vor Sicherheitslücken beitragen. Beispielsweise kann eine neue Version veröffentlicht werden, um Sicherheitsupdates bereitzustellen, Probleme zu beheben oder neue Funktionen einzuführen.

Abhilfe

Informationen zur Migration eines Spark-Jobs zu einer unterstützten Version von AWS Glue finden Sie unter Migration AWS Glue für Spark-Jobs im AWS Glue Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon GuardDuty

Diese AWS Security Hub CSPM Kontrollen bewerten den GuardDuty Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[GuardDuty.1] GuardDuty sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 RA-3 (4), NIST.800-53.r5 SA-11 (1), NIST.800-53.r5 SA-11 (6), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), NIST.800-53.r5 SA-8 (25) NIST.800-53.r5 SC-5,, NIST.800-53.r5 SC-5 (1), NIST.800-53.r5 SC-5 (3) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4 (13), NIST.800-53.r5 SI-4 (2), NIST.800-53.r5 SI-4 (22), NIST.800-53.r5 SI-4 (25), NIST.800-53.r5 SI-4 (4), NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/113.4, PCI DSS v4.0. 1/11.5.1, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.02, CRI-Profil v2. 2/DE. CM-01.03

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: guardduty-enabled-centralized

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Amazon in Ihrem GuardDuty Konto und Ihrer Region aktiviert GuardDuty ist.

Es wird dringend empfohlen, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Auf diese Weise können GuardDuty Sie Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten gewinnen, auch in Regionen, die Sie nicht aktiv nutzen. Dies ermöglicht auch GuardDuty die Überwachung globaler CloudTrail Ereignisse AWS-Services wie IAM.

Abhilfe

Informationen zur Aktivierung GuardDuty finden Sie unter Erste Schritte mit GuardDuty im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Filter`

AWS Config Regel: `tagged-guardduty-filter` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein GuardDuty Amazon-Filter Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Filter keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel

hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Filter mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Filter finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

[GuardDuty.3] GuardDuty IPSets sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::IPSet`

AWS Config Regel: `tagged-guardduty-ipset` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon GuardDuty IPSet Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das IPSet keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das IPSet mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty IPSet finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

[GuardDuty.4] GuardDuty Detektoren sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config Regel: `tagged-guardduty-detector` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Diese Steuerung prüft, ob ein GuardDuty Amazon-Detektor Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Detektor keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Detektor mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Detektor finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/

DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-eks-protection-audit-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty EKS Audit Log Monitoring aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty EKS Audit Log Monitoring im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto EKS Audit Log Monitoring nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die EKS-Audit Log Monitoring-Funktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das GuardDuty EKS Audit Log Monitoring nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty EKS Audit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern zu erkennen. EKS Audit Log Monitoring verwendet Kubernetes-Prüfungsprotokolle, um chronologische Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden und der Steuerebene zu erfassen.

Abhilfe

Informationen zur Aktivierung von GuardDuty EKS Audit Log Monitoring finden Sie unter EKS Audit Log Monitoring im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/115.5.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-lambda-protection-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty Lambda Protection aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty Lambda Protection im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto Lambda Protection nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur für das delegierte Administratorkonto. GuardDuty Nur der delegierte Administrator kann die Lambda Protection-Funktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Dieses Steuerelement generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator über ein gesperrtes Mitgliedskonto verfügt, für das GuardDuty Lambda Protection nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty Lambda Protection hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda Funktion aufgerufen wird. Nachdem Sie Lambda Protection aktiviert haben, GuardDuty beginnt die Überwachung der Lambda-Netzwerkaktivitätsprotokolle, die mit den Lambda-Funktionen in Ihrem verknüpft sind. AWS-Konto Wenn eine Lambda-Funktion aufgerufen wird und verdächtigen Netzwerkverkehr GuardDuty identifiziert, der auf das Vorhandensein eines potenziell bösartigen Codes in Ihrer Lambda-Funktion hinweist, GuardDuty wird ein Befund generiert.

Abhilfe

Informationen zur Aktivierung von GuardDuty Lambda Protection finden Sie unter Konfiguration des Lambda-Schutzes im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/115.5.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-eks-protection-runtime-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty EKS Runtime Monitoring mit automatisierter Agentenverwaltung aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty EKS Runtime Monitoring mit automatisierter Agentenverwaltung im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto EKS Runtime Monitoring mit automatisierter Agentenverwaltung nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Steuerung Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die EKS-Runtime Monitoring-Funktion mit automatisierter Agentenverwaltung für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Dieses Steuerelement generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das GuardDuty EKS Runtime Monitoring nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

EKS Protection in Amazon GuardDuty bietet Schutz vor Bedrohungserkennung, um Sie beim Schutz von Amazon EKS-Clustern in Ihrer AWS Umgebung zu unterstützen. EKS Runtime Monitoring

verwendet Ereignisse auf Betriebssystemebene, um Ihnen zu helfen, potenzielle Bedrohungen in EKS-Knoten und Containern in Ihren EKS-Clustern zu erkennen.

Abhilfe

Informationen zur Aktivierung von EKS Runtime Monitoring mit automatisierter Agentenverwaltung finden Sie unter GuardDuty Enabling Runtime Monitoring im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein

Verwandte Anforderungen: CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/GV. OC-04.03, CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/PR. PS-05.01, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-malware-protection-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der GuardDuty Malware-Schutz aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn der GuardDuty Malware-Schutz im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto der Malware-Schutz nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Steuerelement nur Ergebnisse für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die Malware-Schutzfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty Malware-Schutz nicht aktiviert ist. Um ein `PASSED`

Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty Malware Protection for EC2 hilft Ihnen dabei, das potenzielle Vorhandensein von Malware zu erkennen, indem es die Amazon Elastic Block Store (Amazon EBS) -Volumes scannt, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Container-Workloads angehängt sind. Malware Protection bietet Scanoptionen, mit denen Sie entscheiden können, ob Sie bestimmte EC2-Instances und Container-Workloads beim Scannen ein- oder ausschließen möchten. Es bietet auch die Möglichkeit, die Snapshots von EBS-Volumes, die an die EC2-Instances oder Container-Workloads angehängt sind, in Ihren Konten zu speichern. GuardDuty Die Snapshots werden nur aufbewahrt, wenn Malware gefunden wird und die Erkenntnisse von Malware Protection generiert werden.

Abhilfe

Informationen zur Aktivierung von GuardDuty Malware Protection for EC2 finden Sie unter Konfiguration des GuardDuty-initiated Malware-Scans im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/115.5.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-02.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-rds-protection-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der GuardDuty RDS-Schutz aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn der GuardDuty RDS-Schutz im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto der RDS-Schutz nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle nur Ergebnisse für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die RDS-Schutzfunktion für

die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty RDS-Schutz nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

RDS Protection GuardDuty analysiert und profiliert RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora Aurora-Datenbanken (Aurora MySQL-Compatible Edition und Aurora PostgreSQL-Compatible Edition). Mit dieses Feature können Sie potenziell verdächtiges Anmeldeverhalten identifizieren. RDS Protection erfordert keine zusätzliche Infrastruktur und ist so konzipiert, dass die Leistung Ihrer Datenbank-Instances nicht beeinträchtigt wird. Wenn RDS Protection einen potenziell verdächtigen oder anomalen Anmeldeversuch erkennt, der auf eine Bedrohung für Ihre Datenbank hindeutet, GuardDuty generiert RDS Protection ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank.

Abhilfe

Informationen zur Aktivierung des GuardDuty RDS-Schutzes finden Sie unter GuardDuty RDS-Schutz im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/115.5.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.01, CRI-Profil v2. 2/DE. CM-02.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-s3-protection-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty S3 Protection aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty S3 Protection im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto S3 Protection nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die S3-Schutzfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty S3-Schutz nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

S3 Protection ermöglicht GuardDuty die Überwachung von API-Vorgängen auf Objektebene, um potenzielle Sicherheitsrisiken für Daten in Ihren Amazon Simple Storage Service (Amazon S3) - Buckets zu identifizieren. GuardDuty überwacht Bedrohungen für Ihre S3-Ressourcen, indem AWS CloudTrail Verwaltungsereignisse und CloudTrail S3-Datenereignisse analysiert werden.

Abhilfe

Informationen zur Aktivierung von GuardDuty S3 Protection finden Sie unter Amazon S3 Protection GuardDuty in Amazon im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein

Verwandte Anforderungen: CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Hoch

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-runtime-monitoring-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Runtime Monitoring in Amazon aktiviert ist GuardDuty. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty Runtime Monitoring für das Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn GuardDuty Runtime Monitoring für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto deaktiviert ist.

In einer Umgebung mit mehreren Konten kann nur der delegierte GuardDuty Administrator GuardDuty Runtime Monitoring für Konten in seiner Organisation aktivieren oder deaktivieren. Darüber hinaus kann nur der GuardDuty Administrator die Security Agents konfigurieren und verwalten, die für die Laufzeitüberwachung von AWS Workloads und Ressourcen für Konten in der Organisation GuardDuty verwendet werden. GuardDuty Mitgliedskonten können Runtime Monitoring nicht für ihre eigenen Konten aktivieren, konfigurieren oder deaktivieren.

GuardDuty Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Es verwendet GuardDuty Security Agents, die Einblick in das Laufzeitverhalten, wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen, bieten. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen überwachen möchten, z. B. Amazon EKS-Cluster und Amazon EC2 EC2-Instances.

Abhilfe

Informationen zur Konfiguration und Aktivierung von GuardDuty Runtime Monitoring finden Sie unter GuardDuty Runtime Monitoring and Enabling GuardDuty Runtime Monitoring im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Mittel

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-ecs-protection-runtime-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Amazon GuardDuty Automated Security Agent für die Laufzeitüberwachung von Amazon ECS-Clustern aktiviert ist AWS Fargate. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn der Security Agent für das Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn der Security Agent für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto deaktiviert ist.

In einer Umgebung mit mehreren Konten generiert diese Kontrolle nur Ergebnisse für das delegierte GuardDuty Administratorkonto. Dies liegt daran, dass nur der delegierte GuardDuty Administrator die Laufzeitüberwachung von ECS-Fargate Ressourcen für Konten in seiner Organisation aktivieren oder deaktivieren kann. GuardDuty Mitgliedskonten können dies nicht für ihre eigenen Konten tun. Darüber hinaus generiert dieses Steuerelement `FAILED` Ergebnisse, wenn GuardDuty es für ein Mitgliedskonto gesperrt ist und die Laufzeitüberwachung von ECS-Fargate Ressourcen für das Mitgliedskonto deaktiviert ist. Um einen `PASSED` Befund zu erhalten, muss der GuardDuty Administrator das gesperrte Mitgliedskonto mit GuardDuty dem folgenden Befehl von seinem Administratorkonto trennen.

GuardDuty Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Es verwendet GuardDuty Security Agents, die Einblick in das Laufzeitverhalten, wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen, bieten. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen hin überwachen möchten. Dazu gehören Amazon ECS-Cluster auf AWS Fargate.

Abhilfe

Um den Security Agent für die GuardDuty Laufzeitüberwachung von ECS-Fargate Ressourcen zu aktivieren und zu verwalten, müssen Sie ihn GuardDuty direkt verwenden. Sie können ihn nicht manuell für ECS-Fargate Ressourcen aktivieren oder verwalten. Informationen zur Aktivierung und Verwaltung des Security Agents finden Sie unter Voraussetzungen für den Support AWS Fargate (nur Amazon ECS) und Verwaltung des automatisierten Security Agents für AWS Fargate (nur Amazon ECS) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.01, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-03.02

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Mittel

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config -Regel: guardduty-ec2-protection-runtime-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Steuerung prüft, ob der Amazon GuardDuty Automated Security Agent für die Laufzeitüberwachung von Amazon EC2 EC2-Instances aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn der Security Agent für das Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn der Security Agent für das delegierte GuardDuty Administratorkonto oder ein zugeordnetes Mitgliedskonto deaktiviert ist.

In einer Umgebung mit mehreren Konten generiert diese Kontrolle nur Ergebnisse für das delegierte GuardDuty Administratorkonto. Dies liegt daran, dass nur der delegierte GuardDuty Administrator die Laufzeitüberwachung von Amazon EC2 EC2-Instances für Konten in seiner Organisation aktivieren oder deaktivieren kann. GuardDuty Mitgliedskonten können dies nicht für ihre eigenen Konten tun. Darüber hinaus generiert dieses Steuerelement `FAILED` Ergebnisse, wenn GuardDuty es für ein Mitgliedskonto gesperrt ist und die Laufzeitüberwachung von EC2-Instances für das Mitgliedskonto deaktiviert ist. Um einen `PASSED` Befund zu erhalten, muss der GuardDuty Administrator das gesperrte Mitgliedskonto mit dem folgenden Befehl von seinem Administratorkonto trennen. GuardDuty

GuardDuty Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Es verwendet GuardDuty Security Agents, die Einblick in das Laufzeitverhalten, wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen, bieten. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen hin überwachen möchten. Dies schließt Amazon EC2 EC2-Instances ein.

Abhilfe

Informationen zur Konfiguration und Verwaltung des automatisierten Security Agents für die GuardDuty Laufzeitüberwachung von EC2-Instances finden Sie unter Voraussetzungen für die Unterstützung von Amazon EC2 EC2-Instances und Aktivieren des automatisierten Security Agents für Amazon EC2 EC2-Instances im GuardDuty Amazon-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS Identity and Access Management

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Identity and Access Management (IAM-) Dienst und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/12.2, Benchmark für CIS AWS Foundations v1.4. 0/1.16 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),,, NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.4, PCI DSS v3.2. 1/7.2.1, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: `iam-policy-no-statements-with-admin-access`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy: true`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die Standardversion der IAM-Richtlinien (auch als vom Kunden verwaltete Richtlinien bezeichnet) Administratorzugriff hat. Dazu wird eine Erklärung mit dem Zusatz „`"Effect": "Allow"`mit `"Action": "*"` über`"Resource": "*"`“ hinzugefügt. Die Kontrolle schlägt fehl, wenn Sie über IAM-Richtlinien mit einer solchen Erklärung verfügen.

Das Steuerelement prüft nur die vom Kunden verwalteten Richtlinien, die Sie erstellen. Inline-Richtlinien und AWS verwaltete Richtlinien werden nicht geprüft.

IAM-Richtlinien definieren eine Reihe von Rechten, die Benutzern, Gruppen oder Rollen gewährt werden. Gemäß den üblichen Sicherheitshinweisen wird AWS empfohlen, die geringsten Rechte zu gewähren, d. h., nur die Berechtigungen zu gewähren, die für die Ausführung einer Aufgabe erforderlich sind. Wenn Sie umfassende administrative Berechtigungen anstelle nur derjenigen

bereitstellen, die der Benutzer für seine Tätigkeit benötigt, ermöglichen Sie unter Umständen ungewollte Aktionen mit den Ressourcen.

Anstatt umfassende administrative Berechtigungen zu gewähren, legen Sie fest, was Benutzer tun müssen, und erstellen Sie dann Richtlinien, mit denen die Benutzer nur diese Aufgaben ausführen können. Es ist sicherer, mit einem Mindestsatz von Berechtigungen zu beginnen und bei Bedarf zusätzliche Berechtigungen zu erteilen. Beginnen Sie nicht mit Berechtigungen, die zu weit gefasst sind, und versuchen Sie dann, sie später zu begrenzen.

Sie sollten IAM-Richtlinien entfernen, die eine Erklärung `"Effect": "Allow"` mit der Aufschrift `"Action": "*"` über `"Resource": "*"` enthalten.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen dazu, wie Sie Ihre IAM-Richtlinien so ändern, dass sie keine vollen „*“ - Administratorrechte gewähren, finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.4, Benchmark v3.0 für CIS AWS Foundations. 0/11.5, Benchmark für CIS AWS Foundations v1.2. 0/1.16, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-2, (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-6, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.9, 3.13.3, PCI DSS v3.2. NIST.800-171.r2 1/7.2.1, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-no-policies-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihren IAM-Benutzern Richtlinien zugeordnet sind. Die Kontrolle schlägt fehl, wenn Ihren IAM-Benutzern Richtlinien zugewiesen sind. Stattdessen müssen IAM-Benutzer Berechtigungen von IAM-Gruppen erben oder eine Rolle übernehmen.

Standardmäßig haben IAM-Benutzer, -Gruppen und -Rollen keinen Zugriff auf Ressourcen. AWS IAM-Richtlinien gewähren Benutzern, Gruppen oder Rollen Rechte. Wir empfehlen, dass Sie IAM-Richtlinien direkt auf Gruppen und Rollen anwenden, jedoch nicht auf Benutzer. Das Zuweisen von Berechtigungen auf Gruppen- oder Rollenebene reduziert die Komplexität bei der Zugriffsverwaltung, wenn die Benutzeranzahl steigt. Eine Reduzierung der Komplexität bei der Zugriffsverwaltung kann wiederum das Risiko mindern, dass ein Prinzipal irrtümlicherweise übermäßige Berechtigungen erhält.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie globale Ressourcen nur in einer einzigen Region aufzeichnen, können Sie diese Steuerung in allen Regionen außer der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie eine IAM-Gruppe und hängen Sie die Richtlinie an die Gruppe an. Fügen Sie dann die Benutzer der Gruppe hinzu. Die Richtlinie gilt für jeden Benutzer in der Gruppe. Informationen zum Entfernen einer direkt mit einem Benutzer verknüpften Richtlinie finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.3, Benchmark v3.0 für CIS AWS Foundations. 0/11.4, Benchmark für CIS AWS Foundations v1.4. 0/11.4, Benchmark für CIS

AWS Foundations v1.2. 0/1.4, NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.6.3, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-05.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `access-keys-rotated`

Art des Zeitplans: Periodisch

Parameter:

- `maxAccessKeyAge`: `90` (nicht anpassbar)

Dieses Steuerelement prüft, ob die aktiven Zugriffsschlüssel innerhalb von 90 Tagen rotiert werden.

Wir empfehlen Ihnen dringend, nicht alle Zugriffsschlüssel in Ihrem Konto zu generieren und zu entfernen. Stattdessen empfiehlt es sich, entweder eine oder mehrere IAM-Rollen zu erstellen oder den Verbund über AWS IAM Identity Center zu verwenden. Sie können diese Methoden verwenden, um Ihren Benutzern den Zugriff auf AWS-Managementkonsole und AWS CLI zu ermöglichen.

Jeder Ansatz hat seine Anwendungsfälle. Ein Verbund eignet sich im Allgemeinen besser für Unternehmen, die über ein vorhandenes zentrales Verzeichnis verfügen oder planen, mehr als die aktuelle Anzahl an IAM-Benutzern zu benötigen. Anwendungen, die außerhalb einer AWS Umgebung ausgeführt werden, benötigen Zugriffstasten für den programmatischen Zugriff AWS auf Ressourcen.

Wenn die Ressourcen, die programmatischen Zugriff benötigen, jedoch intern ausgeführt werden AWS, empfiehlt es sich, IAM-Rollen zu verwenden. Rollen ermöglichen es Ihnen, einer Ressource Zugriff zu gewähren, ohne eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel in die Konfiguration zu integrieren.

Weitere Informationen zum Schutz Ihrer Zugriffsschlüssel und Ihres Kontos finden Sie unter Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln in der. Allgemeine AWS-Referenz Lesen Sie auch den Blogbeitrag Richtlinien für Ihren Schutz AWS-Konto bei der Verwendung von programmatischem Zugriff.

Wenn Sie bereits über einen Zugriffsschlüssel verfügen, empfiehlt Security Hub CSPM, die Zugriffsschlüssel alle 90 Tage zu wechseln. Das Rotieren von Zugriffsschlüsseln reduziert die Gefahr,

dass ein Zugriffsschlüssel eines kompromittierten oder gesperrten Kontos verwendet werden kann. Außerdem wird sichergestellt, dass mit einem alten Schlüssel, der möglicherweise verloren gegangen ist, geknackt bzw. gestohlen wurde, nicht auf Daten zugegriffen werden kann. Aktualisieren Sie Ihre Anwendungen immer, nachdem Sie Zugriffsschlüssel rotiert haben.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Sie werden verwendet, um programmatische Anfragen zu signieren, die Sie stellen. AWS Benutzer benötigen ihre eigenen Zugriffsschlüssel, um programmgesteuerte Aufrufe AWS von den Tools for Windows AWS CLI PowerShell, den AWS SDKs oder direkte HTTP-Aufrufe mithilfe der API-Operationen für einzelne Benutzer zu tätigen. AWS-Services

Wenn Ihre Organisation AWS IAM Identity Center (IAM Identity Center) verwendet, können sich Ihre Benutzer bei Active Directory, einem integrierten IAM Identity Center-Verzeichnis oder einem anderen Identitätsanbieter (IdP) anmelden, der mit IAM Identity Center verbunden ist. Sie können dann einer IAM-Rolle zugeordnet werden, die es ihnen ermöglicht, AWS CLI Befehle auszuführen oder AWS API-Operationen aufzurufen, ohne dass Zugriffsschlüssel erforderlich sind. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zur Rotation von Zugriffsschlüsseln, die älter als 90 Tage sind, finden Sie unter Rotieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch. Folgen Sie den Anweisungen für alle Benutzer, deren Zugriffsschlüssel älter als 90 Tage ist.

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.3, Benchmark v3.0 AWS für CIS Foundations. 0/11.4, Benchmark für CIS AWS Foundations v1.4. 0/1.4, Benchmark für CIS AWS Foundations v1.2. 0/11.2, PCI DSS v3.2. 1/2.1, PCI DSS v3.2. 1/22.2, PCI DSS v3.2. 1/7.2.1,

NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), (10) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (2), CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-root-access-key-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Benutzerzugriffsschlüssel vorhanden ist.

Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS-Konto. AWS Zugriffstasten ermöglichen den programmatischen Zugriff auf ein bestimmtes Konto.

Security Hub CSPM empfiehlt, dass Sie alle Zugriffsschlüssel entfernen, die dem Root-Benutzer zugeordnet sind. Dies schränkt die Vektoren ein, die verwendet werden können, um Ihr Konto zu gefährden. Darüber hinaus fördert es die Erstellung und Verwendung rollenbasierter Konten nach dem Prinzip der minimalen Rechte.

Abhilfe

Informationen zum Löschen des Root-Benutzerzugriffsschlüssels finden Sie unter Löschen von Zugriffsschlüsseln für den Root-Benutzer im IAM-Benutzerhandbuch. Informationen zum Löschen der Root-Benutzerzugriffsschlüssel aus einem AWS-Konto IN AWS GovCloud (US) finden Sie unter Löschen der Root-Benutzerzugriffsschlüssel für mein AWS GovCloud (US) Konto im AWS GovCloud (US) Benutzerhandbuch.

[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.9, Benchmark v3.0 für CIS AWS Foundations. 0/11.0, Benchmark für CIS AWS Foundations v1.4. 0/11.0, Benchmark für CIS AWS Foundations v1.2. 0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/8.4.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `mfa-enabled-for-iam-console-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die AWS Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die ein Konsolenkennwort verwenden.

Multi-factor Die Authentifizierung (MFA) bietet zusätzlich zu einem Benutzernamen und einem Passwort eine zusätzliche Schutzebene. Wenn MFA aktiviert ist, wird ein Benutzer, wenn er sich AWS auf einer Website anmeldet, nach seinem Benutzernamen und Passwort gefragt. Darüber hinaus werden sie von ihrem AWS MFA-Gerät zur Eingabe eines Authentifizierungscodes aufgefordert.

Es wird empfohlen, MFA für alle Konten zu aktivieren, die über ein Konsolenpasswort verfügen. MFA wurde entwickelt, um mehr Sicherheit für den Konsolenzugriff zu bieten. Der authentifizierende Prinzipal muss über ein Gerät verfügen, das einen zeitkritischen Schlüssel ausgibt und Kenntnisse über Anmeldeinformationen haben muss.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM-Benutzerhandbuch.

[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.5, Benchmark v3.0 für CIS AWS Foundations. 0/1.6, Benchmark für CIS AWS Foundations v1.4. 0/1.6, Benchmark für CIS AWS Foundations v1.2. 0/11.4, PCI DSS v3.2. 1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/8.4.2, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `root-account-hardware-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob Sie AWS-Konto für die Verwendung eines Hardware-Geräts mit Multi-Faktor-Authentifizierung (MFA) aktiviert sind, um sich mit Root-Benutzeranmeldedaten anzumelden. Die Steuerung schlägt fehl, wenn Hardware-MFA nicht aktiviert ist oder virtuelle MFA-Geräte sich mit Root-Benutzeranmeldedaten anmelden dürfen.

Eine virtuelle MFA bietet möglicherweise nicht das gleiche Sicherheitsniveau wie ein Hardware-MFA-Gerät. Wir empfehlen, dass Sie ein virtuelles MFA-Gerät nur verwenden, solange Sie auf die Genehmigung des Hardwarekaufs oder auf das Eintreffen Ihrer Hardware warten. Weitere Informationen finden Sie unter Zuweisen eines virtuellen MFA-Geräts (Konsole) im IAM-Benutzerhandbuch.

> **Note**
>
> Security Hub CSPM bewertet diese Kontrolle anhand des Vorhandenseins von Root-Benutzeranmeldeinformationen (Anmeldeprofil) in einem. AWS-Konto Die Kontrolle generiert `PASSED` Ergebnisse in den folgenden Fällen:
>
> - Root-Benutzeranmeldeinformationen sind im Konto vorhanden und Hardware-MFA ist für den Root-Benutzer aktiviert.

- Root-Benutzeranmeldedaten sind im Konto nicht vorhanden.

Das Steuerelement generiert einen `FAILED` Befund, wenn Root-Benutzeranmeldedaten im Konto vorhanden sind und Hardware-MFA für den Root-Benutzer nicht aktiviert ist.

Abhilfe

Informationen zur Aktivierung von Hardware-MFA für den Root-Benutzer finden Sie unter Multi-factor Authentifizierung für an Root-Benutzer des AWS-Kontos im IAM-Benutzerhandbuch.

[IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), (15), NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-5 (1), NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/8.3.7, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1, PCI DSS v4.0. 1/83.6.3, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`RequireUppercaseCharacters`	Das Passwort muss mindestens einen Großbuchstaben enthalten	Boolesch	`true` oder `false`	`true`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`RequireLowercaseCharacters`	Das Passwort muss mindestens einen Kleinbuchstaben enthalten	Boolesch	`true` oder `false`	`true`
`RequireSymbols`	Das Passwort muss mindestens ein Symbol enthalten	Boolesch	`true` oder `false`	`true`
`RequireNumbers`	Das Passwort muss mindestens eine Zahl enthalten	Boolesch	`true` oder `false`	`true`
`MinimumPasswordLength`	Mindestanzahl von Zeichen im Passwort	Ganzzahl	8 auf 128	8
`PasswordReusePrevention`	Anzahl der Passwortrotationen, bevor ein altes Passwort wiederverwendet werden kann	Ganzzahl	12 auf 24	Kein Standardwert
`MaxPasswordAge`	Anzahl der Tage bis zum Ablauf des Passworts	Ganzzahl	1 auf 90	Kein Standardwert

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer starke Konfigurationen verwendet. Die Steuerung schlägt fehl, wenn die Kennwortrichtlinie keine starken Konfigurationen verwendet. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, verwendet Security Hub CSPM die in der vorherigen Tabelle genannten Standardwerte. Die `MaxPasswordAge` Parameter `PasswordReusePrevention` und haben keinen Standardwert. Wenn Sie diese Parameter ausschließen, ignoriert Security Hub CSPM bei der Auswertung dieser Steuerung die Anzahl der Kennwortrotationen und das Kennwortalter.

Für den Zugriff auf benötigen AWS-Managementkonsole IAM-Benutzer Passwörter. Als bewährte Methode empfiehlt Security Hub CSPM dringend, anstelle der Erstellung von IAM-Benutzern

den Verbund zu verwenden. Mit dem Verbund können sich Benutzer mit ihren vorhandenen Unternehmensanmeldeinformationen bei der anmelden. AWS-Managementkonsole Verwenden Sie AWS IAM Identity Center (IAM Identity Center), um den Benutzer zu erstellen oder zu verbinden, und übernehmen Sie dann eine IAM-Rolle für ein Konto.

Weitere Informationen zu Identitätsanbietern und Verbund finden Sie unter Identitätsanbieter und Verbund im IAM-Benutzerhandbuch. Weitere Informationen zu IAM Identity Center finden Sie im AWS IAM Identity Center Benutzerhandbuch.

Wenn Sie IAM-Benutzer verwenden müssen, empfiehlt Security Hub CSPM, die Erstellung sicherer Benutzerkennwörter zu erzwingen. Sie können auf Ihrem Computer eine Passwortrichtlinie einrichten, AWS-Konto um die Komplexitätsanforderungen und die obligatorischen Rotationsperioden für Passwörter festzulegen. Wenn Sie eine Kennwortrichtlinie erstellen oder ändern, werden die meisten Einstellungen der Kennwortrichtlinie durchgesetzt, wenn Benutzer ihre Passwörter das nächste Mal ändern. Einige Einstellungen werden sofort durchgesetzt.

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/1.3, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, PCI DSS v3.2. 1/83.1.4, PCI-DSS v4.0. 1/8.2.6, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-05.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-unused-credentials-check`

Art des Zeitplans: Periodisch

Parameter:

- `maxCredentialUsageAge`: `90` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die seit 90 Tagen nicht verwendet wurden.

IAM-Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Passwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

Security Hub CSPM empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 90 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 90 Tage beträgt, sollten Sie die Anmeldeinformationen für diese Benutzer deaktivieren.

Sie können auch Berichte mit Anmeldeinformationen verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 90 oder mehr Tage lang keine Aktivität mehr hatten. Sie können Berichte über Anmeldeinformationen im `.csv` Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts (Konsole).

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.4, PCI DSS v3.2. 1/8.3.1, PCI DSS v4.0. 1/84.4.2, Benchmark v3.0 für CIS AWS Foundations. 0/1.5, Benchmark für CIS AWS Foundations v1.4. 0/1.5, Benchmark für CIS AWS Foundations v1.2. 0/1.13, NIST.800-53.r5 AC-2 (1),

NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `root-account-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Multi-Faktor-Authentifizierung (MFA) aktiviert ist, damit sich der IAM-Root-Benutzer eines bei AWS-Konto dem anmelden kann. AWS-Managementkonsole Die Steuerung schlägt fehl, wenn MFA für den Root-Benutzer des Kontos nicht aktiviert ist.

Der IAM-Root-Benutzer von AWS-Konto hat vollständigen Zugriff auf alle Dienste und Ressourcen im Konto. Wenn MFA aktiviert ist, muss der Benutzer einen Benutzernamen, ein Passwort und einen Authentifizierungscode von seinem AWS MFA-Gerät eingeben, um sich bei dem anzumelden. AWS-Managementkonsole MFA fügt zusätzlich zu einem Benutzernamen und einem Passwort eine zusätzliche Schutzebene hinzu.

Diese Kontrolle generiert `PASSED` Ergebnisse in den folgenden Fällen:

- Root-Benutzeranmeldeinformationen sind im Konto vorhanden und MFA ist für den Root-Benutzer aktiviert.
- Root-Benutzeranmeldedaten sind im Konto nicht vorhanden.

Das Steuerelement generiert `FAILED` Ergebnisse, wenn Root-Benutzeranmeldeinformationen im Konto vorhanden sind und MFA für den Root-Benutzer nicht aktiviert ist.

Abhilfe

Informationen zur Aktivierung von MFA für den Root-Benutzer eines AWS-Konto finden Sie unter Multi-factor Authentifizierung für den Root-Benutzer des AWS-Kontos im AWS Identity and Access Management Benutzerhandbuch.

[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

Verwandte Anforderungen: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v3.2. 1/81.1.4, PCI DSS v3.2. 1/8.2.3, PCI-DSS v3.2. 1/8.2.4, PCI DSS v3.2. 1/8.2.5, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer die folgenden PCI-DSS-Mindestkonfigurationen verwendet.

- `RequireUppercaseCharacters`— Das Passwort muss mindestens einen Großbuchstaben enthalten. (Standardwert = `true`)
- `RequireLowercaseCharacters`— Das Passwort muss mindestens einen Kleinbuchstaben enthalten. (Standardwert = `true`)
- `RequireNumbers`— Erfordert mindestens eine Zahl im Passwort. (Standardwert = `true`)
- `MinimumPasswordLength`— Mindestlänge des Passworts. (Standard = 7 oder länger)
- `PasswordReusePrevention`— Anzahl der Passwörter vor der Wiederverwendung. (Standard = 4)
- `MaxPasswordAge`— Anzahl der Tage bis zum Ablauf des Passworts. (Standard = 90)

> **Note**
>
> Am 30. Mai 2025 entfernte Security Hub CSPM diese Steuerung aus dem PCI DSS v4.0.1-Standard. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Diese Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten.

Um die Kennwortrichtlinien für Konten anhand der Anforderungen von PCI DSS v4.0.1 zu bewerten, können Sie das Steuerelement verwenden. IAM.7 Für dieses Steuerelement müssen Kennwörter mindestens 8 Zeichen lang sein. Es unterstützt auch benutzerdefinierte Werte für die Passwortlänge und andere Parameter. Die IAM.7 Steuerung ist Teil des PCI DSS v4.0.1-Standards in Security Hub CSPM.

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie zur Verwendung der empfohlenen Konfiguration finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch.

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/13.5, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/83.6.3, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Passwortrichtlinie mindestens einen Großbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Großbuchstaben des lateinischen Alphabets erforderlich (A—Z) aus.

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/13.6, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/83.6.3, CRI-Profil v2. 2/PR. AA-01.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden. CIS empfiehlt, dass die Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Kleinbuchstaben des lateinischen Alphabets erforderlich (A—Z) aus.

[IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/11.7, NIST.800-171.r2 3.5.7, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Passwortrichtlinie mindestens ein Symbol erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens ein nichtalphanumerisches Zeichen erforderlich aus.

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/11.8, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/83.3.6, PCI DSS v4.0. 1/83.6.3, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Passwortrichtlinie mindestens eine Zahl erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens eine Zahl erforderlich aus.

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.7, Benchmark v3.0 für CIS AWS Foundations. 0/1.8, Benchmark für CIS AWS Foundations v1.4. 0/1.8, Benchmark für CIS AWS Foundations v1.2. 0/1.9, NIST.800-171.r2 3.5.7, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter mindestens eine bestimmte Länge haben.

CIS empfiehlt, dass die Passwortrichtlinie eine Mindestkennwortlänge von 14 Zeichen vorschreibt. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Passwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie als Mindestlänge für das Passwort eine **14** oder eine größere Zahl ein.

[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/1.8, Benchmark v3.0 für CIS AWS Foundations. 0/1.9, Benchmark für CIS AWS Foundations v1.4. 0/1.9, Benchmark für CIS AWS Foundations v1.2. 0/11.0, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/83.3.7, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob die Anzahl der Passwörter, die Sie sich merken müssen, auf 24 gesetzt ist. Die Steuerung schlägt fehl, wenn der Wert nicht 24 ist.

IAM-Passwortrichtlinien können die Wiederverwendung eines bestimmten Passworts durch denselben Benutzer verhindern.

CIS empfiehlt, dass die Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert. Das Verhindern der Wiederverwendung von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie für „Wiederverwendung von Passwörtern verhindern“ ein. **24**

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/11.1, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

IAM-Passwortrichtlinien können vorschreiben, dass Passwörter nach einer bestimmten Anzahl von Tagen ausgetauscht werden oder abgelaufen sind.

CIS empfiehlt, dass die Passwortrichtlinie Passwörter nach 90 Tagen oder weniger abläuft. Das Reduzieren der Lebensdauer von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche. Darüber hinaus ist es in folgenden Situationen hilfreich, wenn regelmäßige Passwortänderungen gefordert werden:

- Passwörter können ohne Ihr Wissen gestohlen oder kompromittiert werden. Dies kann durch eine Systemkompromittierung, eine Softwareschwachstelle oder eine interne Bedrohung erfolgen.
- Bestimmte Web-Filter oder Proxy-Server von Unternehmen und Behörden können Datenverkehr abfangen und erfassen, selbst wenn er verschlüsselt ist.
- Viele Menschen verwenden dasselbe Passwort für viele Systeme, z. B. für die Arbeit, E-Mails und den privaten Gebrauch.
- Auf kompromittierten Endbenutzer-Workstations kann ein Keylogger vorhanden sein.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie für „Ablauf des Kennworts aktivieren“ eine kleinere **`90`** Zahl oder ein.

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.6, Benchmark v3.0 für CIS AWS Foundations. 0/11.7, Benchmark für CIS AWS Foundations v1.4. 0/11.7, Benchmark für CIS AWS Foundations v1.2. 0/12.0, NIST.800-171.r2 3.1.2, PCI DSS v4.0. 1/122.10.3, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-policy-in-use`

Art des Zeitplans: Periodisch

Parameter:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess` (nicht anpassbar)
- `policyUsageType`: `ANY` (nicht anpassbar)

AWS bietet ein Support-Center, das für die Benachrichtigung und Reaktion auf Vorfälle sowie für technischen Support und Kundendienst genutzt werden kann.

Erstellen Sie eine IAM-Rolle, damit autorisierte Benutzer Vorfälle mit AWS Support verwalten können. Durch die Implementierung von Least-Privilegien für die Zugriffskontrolle erfordert eine IAM-Rolle eine entsprechende IAM-Richtlinie, die den Zugriff auf das Supportcenter ermöglicht, damit Vorfälle bearbeitet werden können. Support

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie eine Rolle, die es autorisierten Benutzern ermöglicht, Support Vorfälle zu verwalten.

Um die Rolle zu erstellen, für die verwendet werden soll Support access

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im IAM-Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie als Rollentyp die Option Andere AWS-Konto aus.
4. Geben Sie unter Konto-ID die AWS-Konto ID der AWS-Konto Person ein, der Sie Zugriff auf Ihre Ressourcen gewähren möchten.

   Wenn sich die Benutzer oder Gruppen, die diese Rolle übernehmen, im selben Konto befinden, geben Sie die lokale Kontonummer ein.

   > **Note**
   >
   > Der Administrator des angegebenen Kontos kann die Berechtigung erteilen, diese Rolle für alle -Benutzer in diesem Konto zu übernehmen. Hierzu fügt der Administrator eine Richtlinie an den Benutzer oder eine Gruppe an, mit der die Berechtigung für die Aktion `sts:AssumeRole` gewährt wird. In dieser Richtlinie muss die Ressource der Rollen-ARN sein.

5. Wählen Sie Weiter: Berechtigungen aus.
6. Suchen Sie nach der verwalteten Richtlinie `AWSSupportAccess`.
7. Wählen Sie das Kontrollkästchen für die verwaltete `AWSSupportAccess`-Richtlinie aus.
8. Wählen Sie Weiter: Tags aus.
9. (Optional) Um der Rolle Metadaten hinzuzufügen, fügen Sie Tags als Schlüssel-Wert-Paare hinzu.

   Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tagging von IAM-Benutzern und -Rollen im IAM-Benutzerhandbuch.
10. Klicken Sie auf Next: Review (Weiter: Prüfen).
11. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein.

Rollennamen müssen innerhalb Ihrer eindeutig sein. AWS-Konto Sie unterscheiden nicht zwischen Groß- und Kleinschreibung.

12. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die neue Rolle ein.
13. Prüfen Sie die Rolle und klicken Sie dann auf Create role (Rolle erstellen).

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.5.3, NIST.800-171.r2 3.5.4, 3.7.5, PCI DSS NIST.800-171.r2 v3.2. 1/83.3.1, PCI DSS v4.0. 1/8.4.2, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die IAM-Benutzer die Multi-Faktor-Authentifizierung (MFA) aktiviert haben.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter Aktivieren von MFA-Geräten für Benutzer AWS im IAM-Benutzerhandbuch.

[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers

> **Important**
>
> Security Hub CSPM hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub CSPM-Steuerelemente.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2. 0/11.

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: `use-of-root-account-test` (benutzerdefinierte Security Hub CSPM-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für an AWS-Konto Beschränkungen für die Nutzung des Root-Benutzers gelten. Das Steuerelement bewertet die folgenden Ressourcen:

- Amazon Simple Notification Service (Amazon SNS)-Themen
- AWS CloudTrail Pfade
- Mit den CloudTrail Pfaden verknüpfte metrische Filter
- CloudWatch Amazon-Alarme basierend auf den Filtern

Bei dieser Prüfung wird `FAILED` festgestellt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Auf dem Konto sind keine CloudTrail Spuren vorhanden.
- Ein CloudTrail Trail ist aktiviert, aber nicht mit mindestens einem Trail für mehrere Regionen konfiguriert, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst.

- Ein CloudTrail Trail ist aktiviert, aber keiner CloudWatch Logs-Protokollgruppe zugeordnet.
- Der vom Center for Internet Security (CIS) vorgeschriebene exakte metrische Filter wird nicht verwendet. Der vorgeschriebene metrische Filter ist`'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- In dem Konto sind keine CloudWatch Alarme vorhanden, die auf dem metrischen Filter basieren.
- CloudWatch Alarme, die so konfiguriert sind, dass sie Benachrichtigungen an das zugehörige SNS-Thema senden, werden nicht aufgrund der Alarmbedingung ausgelöst.
- Das SNS-Thema entspricht nicht den Einschränkungen für das Senden einer Nachricht an ein SNS-Thema.
- Das SNS-Thema hat nicht mindestens einen Abonnenten.

Diese Prüfung führt zu einem Kontrollstatus, der `NO_DATA` angibt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub CSPM kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub CSPM kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Diese Prüfung führt zu einem Kontrollstatus, der angibt`WARNING`, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Das aktuelle Konto ist nicht Eigentümer des SNS-Themas, auf das in der CloudWatch Warnung verwiesen wird.
- Das Girokonto hat beim Aufrufen der SNS-API keinen Zugriff auf das SNS-Thema. `ListSubscriptionsByTopic`

> **Note**
>
> Wir empfehlen, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern ausgewertet wurden. In Mitgliedskonten generiert Security Hub

CSPM nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-CSPM-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Es hat sich bewährt, Ihre Root-Benutzeranmeldedaten nur dann zu verwenden, wenn dies für die Konto- und Serviceverwaltung erforderlich ist. Wenden Sie IAM-Richtlinien direkt auf Gruppen und Rollen an, jedoch nicht auf Benutzer. Anweisungen zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe.

Abhilfe

Zu den Schritten zur Behebung dieses Problems gehören die Einrichtung eines Amazon SNS SNS-Themas, eines CloudTrail Trails, eines Metrikfilters und eines Alarms für den Metrikfilter.

Erstellen eines Amazon SNS-Themas

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Erstellen Sie ein Amazon SNS SNS-Thema, das alle CIS-Alarme empfängt.

   Erstellen Sie mindestens einen Abonnenten für das Thema. Weitere Informationen finden Sie unter Erste Schritte mit Amazon SNS im Benutzerhandbuch für Amazon Simple Notification Service.

Richten Sie als Nächstes eine aktive Option ein CloudTrail , die für alle Regionen gilt. Um dies zu tun, befolgen Sie die Schritte in the section called “[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst”.

Notieren Sie sich den Namen der Protokollgruppe CloudWatch Logs, die Sie dem CloudTrail Trail zuordnen. Sie erstellen den Metrikfilter für diese Protokollgruppe.

Erstellen Sie abschließend den metrischen Filter und den Alarm.

Erstellen eines Metrikfilters und Alarms

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe CloudWatch Logs, die dem von Ihnen erstellten CloudTrail Trail zugeordnet ist.
4. Wählen Sie unter Aktionen die Option Metrikfilter erstellen aus.
5. Gehen Sie unter Muster definieren wie folgt vor:

   a. Kopieren Sie das folgende Muster und fügen Sie es dann in das Feld Filter Pattern (Filtermuster) ein.

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. Wählen Sie Weiter aus.
6. Gehen Sie unter Metrik zuweisen wie folgt vor:

   a. Geben Sie im Feld Filtername einen Namen für Ihren Metrikfilter ein.

   b. Geben **`LogMetrics`** Sie für Metric Namespace den Wert ein.

      Wenn Sie denselben Namespace für alle Ihre CIS-Log-Metrikfilter verwenden, werden alle CIS-Benchmark-Metriken zusammen gruppiert.

   c. Geben Sie unter Metrikname einen Namen für die Metrik ein. Merken Sie sich den Namen der Metrik. Sie müssen die Metrik auswählen, wenn Sie den Alarm erstellen.

   d. Geben Sie für Metric value (Metrikwert) **1** ein.

   e. Wählen Sie Weiter aus.
7. Überprüfen Sie unter Überprüfen und erstellen die Informationen, die Sie für den neuen Metrikfilter angegeben haben. Wählen Sie dann Metrikfilter erstellen aus.
8. Wählen Sie im Navigationsbereich Protokollgruppen und dann den Filter aus, den Sie unter Metrikfilter erstellt haben.
9. Aktivieren Sie das Kontrollkästchen für den Filter. Wählen Sie Alarm erstellen aus.
10. Gehen Sie unter Metrik und Bedingungen angeben wie folgt vor:

    a. Wählen Sie unter Bedingungen für Schwellenwert die Option Statisch aus.

    b. Wählen Sie unter Alarmbedingung definieren die Option Greater/Equal.

    c. Geben Sie unter Schwellenwert definieren den Wert ein**1**.

    d. Wählen Sie Weiter aus.

11. Gehen Sie unter Aktionen konfigurieren wie folgt vor:
    a. Wählen Sie unter Auslöser für den Alarmstatus die Option Bei Alarm aus.
    b. Wählen Sie unter Select an SNS topic (SNS-Thema auswählen) die Option Select an existing SNS topic (Vorhandenes SNS-Thema auswählen) aus.
    c. Geben Sie unter Benachrichtigung senden an den Namen des SNS-Themas ein, das Sie im vorherigen Verfahren erstellt haben.
    d. Wählen Sie Weiter aus.
12. Geben Sie unter Namen und Beschreibung hinzufügen einen Namen und eine Beschreibung für den Alarm ein, z. B. **`CIS-1.1-RootAccountUsage`** Klicken Sie anschließend auf Weiter.
13. Überprüfen Sie unter Vorschau und Erstellung die Alarmkonfiguration. Wählen Sie anschließend Create alarm (Alarm erstellen) aus.

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5, (2) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.1, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.5, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.3.9, 3.13.3, 3.13.4, CRI Profile v2. NIST.800-171.r2 NIST.800-171.r2 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Erkennen > Sicheres Zugriffsmanagement

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: `iam-policy-no-statements-with-full-access`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy`: `True` (nicht anpassbar)

Dieses Steuerelement prüft, ob die identitätsbasierten IAM-Richtlinien, die Sie erstellen, über Allow-Anweisungen verfügen, die den Platzhalter „*“ verwenden, um Berechtigungen für alle Aktionen in

einem Dienst zu gewähren. Das Steuerelement schlägt fehl, wenn eine Richtlinienanweisung mit enthält. `"Effect": "Allow"` `"Action": "Service:*"`

Beispielsweise führt die folgende Aussage in einer Richtlinie zu einem fehlgeschlagenen Ergebnis.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Das Steuerelement schlägt auch fehl, wenn Sie `"Effect": "Allow"` mit verwenden`"NotAction": "service:*"`. In diesem Fall bietet das `NotAction` Element Zugriff auf alle Aktionen in einem AWS-Service, mit Ausnahme der in angegebenen Aktionen`NotAction`.

Diese Kontrolle gilt nur für vom Kunden verwaltete IAM-Richtlinien. Sie gilt nicht für IAM-Richtlinien, die von verwaltet werden. AWS

Wenn Sie Berechtigungen zuweisen AWS-Services, ist es wichtig, dass Sie den Umfang der zulässigen IAM-Aktionen in Ihren IAM-Richtlinien angeben. Sie sollten IAM-Aktionen nur auf die Aktionen beschränken, die benötigt werden. Auf diese Weise können Sie Berechtigungen mit den geringsten Rechten bereitstellen. Zu freizügige Richtlinien können zu einer Eskalation von Rechten führen, wenn die Richtlinien einem IAM-Prinzipal zugeordnet sind, für den die Genehmigung möglicherweise nicht erforderlich ist.

In einigen Fällen möchten Sie möglicherweise IAM-Aktionen zulassen, die ein ähnliches Präfix haben, z. B. und. `DescribeFlowLogs` `DescribeAvailabilityZones` In diesen autorisierten Fällen können Sie dem allgemeinen Präfix einen Platzhalter mit einem Suffix hinzufügen. Beispiel, `ec2:Describe*`.

Dieses Steuerelement ist erfolgreich, wenn Sie eine IAM-Aktion mit einem Präfix und einem Platzhalter mit Suffix verwenden. Beispielsweise führt die folgende Anweisung in einer Richtlinie zu einem erfolgreichen Ergebnis.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
```

```
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Wenn Sie verwandte IAM-Aktionen auf diese Weise gruppieren, können Sie auch verhindern, dass die Größenbeschränkungen der IAM-Richtlinie überschritten werden.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre IAM-Richtlinien, sodass sie keine vollen „*“ -Administratorrechte zulassen. Einzelheiten zur Bearbeitung einer IAM-Richtlinie finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.1, Benchmark v3.0 für CIS AWS Foundations. 0/11.2, Benchmark für CIS AWS Foundations v1.4. 0/1.12, NIST.800-171.r2 3.1.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-05.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: **`iam-user-unused-credentials-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die 45 Tage oder länger nicht verwendet wurden. Zu diesem Zweck wird geprüft, ob der `maxCredentialUsageAge` Parameter der AWS Config Regel 45 oder mehr beträgt.

Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Kennwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

CIS empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 45 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

Die AWS Config Regel für dieses Steuerelement verwendet die Operationen `GetCredentialReport`und `GenerateCredentialReport`API, die nur alle vier Stunden aktualisiert werden. Es kann bis zu vier Stunden dauern, bis Änderungen an IAM-Benutzern für dieses Steuerelement sichtbar sind.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub CSPM verwenden. Sie können jedoch die Aufzeichnung globaler Ressourcen in einer einzigen Region aktivieren. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 45 Tage beträgt, deaktivieren Sie die Anmeldeinformationen für diese Benutzer.

Sie können auch Berichte über Anmeldeinformationen verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 45 oder mehr Tage lang keine Aktivität hatten. Sie können Berichte über Anmeldeinformationen im `.csv` Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts (Konsole).

[IAM.23] IAM Access Analyzer-Analyzer sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AccessAnalyzer::Analyzer`

AWS Config Regel: `tagged-accessanalyzer-analyzer` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein von AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) verwalteter Analyzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Analyzer keine Tagschlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Analyzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Analyzer finden Sie TagResourcein der AWS IAM Access Analyzer API-Referenz.

[IAM.24] IAM-Rollen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::Role`

AWS Config Regel: `tagged-iam-role` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine AWS Identity and Access Management (IAM-) Rolle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Rolle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Rolle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer IAM-Rolle finden Sie unter Tagging IAM-Ressourcen im IAM-Benutzerhandbuch.

[IAM.25] IAM-Benutzer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: `tagged-iam-user` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS Identity and Access Management (IAM-) Benutzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Benutzer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Benutzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IAM-Benutzer finden Sie unter Tagging IAM-Ressourcen im IAM-Benutzerhandbuch.

[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.8, Benchmark v3.0 für CIS AWS Foundations. 0/1.19, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Identifizieren > Konformität

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::ServerCertificate`

AWS Config Regel: **`iam-server-certificate-expiration-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Steuerung wird geprüft, ob ein aktives SSL/TLS Serverzertifikat, das in IAM verwaltet wird, abgelaufen ist. Die Kontrolle schlägt fehl, wenn das abgelaufene SSL/TLS Serverzertifikat nicht entfernt wird.

Um HTTPS-Verbindungen zu Ihrer Website oder Anwendung in zu aktivieren AWS, benötigen Sie ein SSL/TLS Serverzertifikat. Sie können IAM oder AWS Certificate Manager (ACM) verwenden, um Serverzertifikate zu speichern und bereitzustellen. Verwenden Sie IAM nur dann als Zertifikatsmanager, wenn Sie HTTPS-Verbindungen in einer Umgebung unterstützen müssen AWS-Region , die von ACM nicht unterstützt wird. IAM bietet eine sichere Verschlüsselungsmethode für Ihre privaten Schlüssel und speichert die verschlüsselte Version in einem SSL-Zertifikatspeicher in IAM. IAM unterstützt die Bereitstellung von Serverzertifikaten in allen Regionen, Sie müssen Ihr Zertifikat jedoch von einem externen Anbieter beziehen, damit Sie es verwenden können. AWS Sie können kein ACM-Zertifikat auf IAM hochladen. Darüber hinaus können Sie Ihre Zertifikate nicht von der IAM-Konsole aus verwalten. Durch das Entfernen abgelaufener SSL/TLS Zertifikate wird das Risiko vermieden, dass versehentlich ein ungültiges Zertifikat für eine Ressource bereitgestellt wird, wodurch die Glaubwürdigkeit der zugrunde liegenden Anwendung oder Website beeinträchtigt werden kann.

Abhilfe

Informationen zum Entfernen eines Serverzertifikats aus IAM finden Sie unter Verwalten von Serverzertifikaten in IAM im IAM-Benutzerhandbuch.

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/12.1, Benchmark v3.0 für CIS AWS Foundations. 0/12.2, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Sichere IAM-Richtlinien

Schweregrad: Mittel

Ressourcentyp:`AWS::IAM::Role`,, `AWS::IAM::User` `AWS::IAM::Group`

AWS Config Regel: **`iam-policy-blacklisted-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- „policyArns“: „arn:aws:iam: :aws:, arn:aws-cn:iam: :aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam: :aws:“ policy/AWSCloudShellFullAccess policy/AWSCloudShellFullAccess

Dieses Steuerelement prüft, ob eine IAM-Identität (Benutzer, Rolle oder Gruppe) mit der verwalteten Richtlinie verknüpft ist. AWS `AWSCloudShellFullAccess` Die Steuerung schlägt fehl, wenn die `AWSCloudShellFullAccess` Richtlinie an eine IAM-Identität angehängt ist.

AWS CloudShell bietet eine bequeme Möglichkeit, CLI-Befehle auszuführen AWS-Services. Die AWS verwaltete Richtlinie `AWSCloudShellFullAccess` bietet vollen Zugriff CloudShell auf und ermöglicht somit das Hoch- und Herunterladen von Dateien zwischen dem lokalen System eines Benutzers und der CloudShell Umgebung. Innerhalb der CloudShell Umgebung verfügt ein Benutzer über Sudo-Berechtigungen und kann auf das Internet zugreifen. Das Anhängen dieser verwalteten Richtlinie an eine IAM-Identität gibt ihnen somit die Möglichkeit, Dateiübertragungssoftware zu installieren und Daten von externen Internetservern CloudShell zu verschieben. Wir empfehlen, dem Prinzip der geringsten Rechte zu folgen und Ihren IAM-Identitäten engere Berechtigungen zuzuweisen.

Abhilfe

Informationen zum Trennen der *`AWSCloudShellFullAccess`* Richtlinie von einer IAM-Identität finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

[IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/11.9, Benchmark v3.0 für CIS AWS Foundations. 0/1.20, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. AA-05.04

Kategorie: Erkennen > Erkennungsdienste > Überwachung privilegierter Nutzung

Schweregrad: Hoch

Art der Ressource: `AWS::AccessAnalyzer::Analyzer`

AWS Config Regel: **`iam-external-access-analyzer-enabled`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS-Konto ein externer Zugriffsanalysator für IAM Access Analyzer aktiviert ist. Die Steuerung schlägt fehl, wenn für das Konto in Ihrem aktuell ausgewählten AWS-Region Konto kein External Access Analyzer aktiviert ist.

Die externen Zugriffsanalysatoren von IAM Access Analyzer helfen dabei, Ressourcen wie Amazon Simple Storage Service (Amazon S3) -Buckets oder IAM-Rollen zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Auf diese Weise können Sie einen unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten vermeiden. IAM Access Analyzer ist regional und muss in jeder Region aktiviert sein. Um Ressourcen zu identifizieren, die gemeinsam mit externen Principals genutzt werden, analysiert ein Access Analyzer die ressourcenbasierten Richtlinien in Ihrer Umgebung anhand von logischen Argumenten. AWS Wenn Sie einen externen Zugriffsanalysator erstellen, können Sie ihn für Ihr gesamtes Unternehmen oder für einzelne Konten erstellen und aktivieren.

> **Note**
>
> Wenn ein Konto Teil einer Organisation in ist AWS Organizations, werden externe Zugriffsanalysatoren, die die Organisation als Vertrauenszone angeben und für die Organisation in der aktuellen Region aktiviert sind, bei dieser Steuerung nicht berücksichtigt. Wenn Ihre Organisation diese Art von Konfiguration verwendet, sollten Sie erwägen, diese Steuerung für einzelne Mitgliedskonten in Ihrer Organisation in der Region zu deaktivieren.

Abhilfe

Informationen zur Aktivierung eines externen Access Analyzers in einer bestimmten Region finden Sie unter Erste Schritte mit IAM Access Analyzer im IAM-Benutzerhandbuch. Sie müssen in jeder Region, in der Sie den Zugriff auf Ihre Ressourcen überwachen möchten, einen Analyzer aktivieren.

Security Hub CSPM-Steuerungen für Amazon Inspector

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Inspector.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/113.3.1, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `inspector-ec2-scan-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Amazon Inspector EC2-Scannen aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Amazon Inspector EC2-Scannen im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto oder ein zugeordnetes Mitgliedskonto das EC2-Scannen nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die EC2-Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte Administrator ein gesperrtes Mitgliedskonto hat, für das der Amazon Inspector EC2-Scan nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Das Amazon Inspector EC2-Scannen extrahiert Metadaten aus Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance und vergleicht diese Metadaten dann mit Regeln, die in Sicherheitsempfehlungen gesammelt wurden, um Ergebnisse zu erzielen. Amazon Inspector scannt Instances auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Informationen zu unterstützten Betriebssystemen, einschließlich der Betriebssysteme, die ohne SSM-Agent gescannt werden können, finden Sie unter Unterstützte Betriebssysteme: Amazon EC2-Scannen.

Abhilfe

Informationen zum Aktivieren von Amazon Inspector EC2-Scans finden Sie unter Aktivieren von Scans im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/113.3.1, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `inspector-ecr-scan-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Amazon Inspector ECR-Scannen aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Amazon Inspector ECR-Scannen im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto oder ein zugeordnetes Mitgliedskonto kein ECR-Scan aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die ECR-Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte Administrator über ein gesperrtes Mitgliedskonto verfügt, für das der Amazon Inspector ECR-Scan nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Amazon Inspector scannt Container-Images, die in Amazon Elastic Container Registry (Amazon ECR) gespeichert sind, auf Softwareschwachstellen, um Sicherheitslücken in Paketen zu ermitteln. Wenn Sie Amazon Inspector-Scans für Amazon ECR aktivieren, legen Sie Amazon Inspector als

Ihren bevorzugten Scan-Service für Ihre private Registrierung fest. Dadurch wird das einfache Scannen, das von Amazon ECR kostenlos bereitgestellt wird, durch das erweiterte Scannen ersetzt, das über Amazon Inspector bereitgestellt und in Rechnung gestellt wird. Das erweiterte Scannen bietet Ihnen den Vorteil des Schwachstellenscans sowohl für Betriebssysteme als auch für Programmiersprachenpakete auf Registrierungsebene. Sie können die Ergebnisse, die mit dem erweiterten Scannen auf Bildebene entdeckt wurden, für jede Ebene des Bilds in der Amazon ECR-Konsole überprüfen. Darüber hinaus können Sie diese Ergebnisse in anderen Diensten überprüfen und mit ihnen arbeiten, die für grundlegende Scanergebnisse nicht verfügbar sind, einschließlich AWS Security Hub CSPM Amazon EventBridge.

Abhilfe

Informationen zum Aktivieren von Amazon Inspector ECR-Scans finden Sie unter Aktivieren von Scans im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/6.2.4, PCI DSS v4.0. 1/6.3.1, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `inspector-lambda-code-scan-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Scannen von Amazon Inspector Lambda-Code aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Scannen von Amazon Inspector Lambda-Code im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto oder ein zugeordnetes Mitgliedskonto der Lambda-Code-Scan nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die Lambda-Code-

Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte Administrator ein gesperrtes Mitgliedskonto hat, für das Amazon Inspector Lambda-Code-Scan nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Das Amazon Inspector Lambda-Codescanning scannt den benutzerdefinierten Anwendungscode innerhalb einer AWS Lambda Funktion auf Code-Schwachstellen auf der Grundlage bewährter AWS Sicherheitsmethoden. Durch das Scannen von Lambda-Code können Injektionsfehler, Datenlecks, schwache Kryptografie oder fehlende Verschlüsselung in Ihrem Code erkannt werden. Diese Funktion ist nur in bestimmten AWS-Regionen Fällen verfügbar. Sie können das Lambda-Code-Scannen zusammen mit dem Lambda-Standardscannen aktivieren (siehe[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein).

Abhilfe

Informationen zur Aktivierung des Amazon Inspector Lambda-Code-Scans finden Sie unter Aktivieren von Scans im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/6.2.4, PCI DSS v4.0. 1/6.3.1, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `inspector-lambda-standard-scan-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Standardscannen von Amazon Inspector Lambda aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn der Amazon Inspector Lambda-Standardscan im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die

Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto oder ein zugeordnetes Mitgliedskonto das Lambda-Standardscannen nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die Lambda-Standardscanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert `FAILED` Ergebnisse, wenn der delegierte Administrator ein gesperrtes Mitgliedskonto hat, für das Amazon Inspector Lambda Standard-Scan nicht aktiviert ist. Um ein `PASSED` Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Das Standard-Scannen von Amazon Inspector Lambda identifiziert Softwareschwachstellen in den Abhängigkeiten von Anwendungspaketen, die Sie Ihrem AWS Lambda Funktionscode und Ihren Ebenen hinzufügen. Wenn Amazon Inspector eine Sicherheitslücke in den Abhängigkeiten Ihrer Lambda-Funktionsanwendung feststellt, erstellt Amazon Inspector eine detaillierte `Package Vulnerability` Typfindung. Sie können das Lambda-Code-Scannen zusammen mit dem Lambda-Standardscannen aktivieren (siehe[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein).

Abhilfe

Informationen zur Aktivierung von Amazon Inspector Lambda-Standardscans finden Sie unter Aktivieren von Scans im Amazon Inspector Inspector-Benutzerhandbuch.

Security Hub CSPM-Steuerungen fürAWS IoT

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS IoT Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbarAWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::SecurityProfile`

AWS ConfigRegel: `tagged-iot-securityprofile` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS IoT Device Defender Sicherheitsprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Sicherheitsprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Sicherheitsprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Device Defender Sicherheitsprofil finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::MitigationAction`

AWS ConfigRegel: `tagged-iot-mitigationaction` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		AWSAnforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine AWS IoT Core Schadensbegrenzungsaktion über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Abhilfemaßnahme keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Abhilfemaßnahme mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Schadensbegrenzungsmaßnahme finden Sie unter Taggen Ihrer AWS IoT Ressourcen im Entwicklerhandbuch. AWS IoT

[IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Dimension`

AWS ConfigRegel: `tagged-iot-dimension` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine AWS IoT Core Dimension über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Dimension keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Dimension mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Dimension finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.4]AWS IoT CoreAutorisierer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Authorizer`

AWS ConfigRegel: `tagged-iot-authorizer` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS IoT Core Autorisierer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Autorisierer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Autorisierer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Autorisierer finden Sie unter Taggen Ihrer AWS IoT Ressourcen im Entwicklerhandbuch. AWS IoT

[IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::RoleAlias`

AWS ConfigRegel: `tagged-iot-rolealias` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS IoT Core Rollenalias Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Rollenalias keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Rollenalias mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Rollenalias finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Policy`

AWS ConfigRegel: `tagged-iot-policy` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine AWS IoT Core Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Richtlinie finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

Security Hub CSPM-Steuerungen fürAWSIoT SiteWise

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS SiteWise IoT-Dienst und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbarAWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::AssetModel`

AWS Config-Regel: `iotsitewise-asset-model-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Asset-Modell Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Asset-Modell keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Asset-Modell mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Assetmodell finden Sie unter Taggen Ihrer AWS IoT SiteWise Ressourcen im AWS IoT SiteWiseBenutzerhandbuch.

[IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Dashboard`

AWS Config-Regel: `iotsitewise-dashboard-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Dashboard Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Dashboard keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Dashboard mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Dashboard finden Sie unter Taggen Ihrer AWS IoT SiteWise Ressourcen im AWS IoT SiteWiseBenutzerhandbuch.

[IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Gateway`

AWS Config-Regel: `iotsitewise-gateway-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Gateway über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Gateway finden Sie unter Taggen Ihrer AWS IoT SiteWise Ressourcen im AWS IoT SiteWiseBenutzerhandbuch.

[IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Portal`

AWS Config-Regel: `iotsitewise-portal-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		AWSAnforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Portal Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Portal keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Portal mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services,

darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Portal finden Sie unter Taggen Ihrer AWS IoT SiteWise Ressourcen im AWS IoT SiteWiseBenutzerhandbuch.

[IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Project`

AWS Config-Regel: `iotsitewise-project-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Projekt Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Projekt keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel

hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Projekt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Projekt finden Sie unter Taggen Ihrer AWS IoT SiteWise Ressourcen im AWS IoT SiteWiseBenutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS IoT TwinMaker

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS TwinMaker IoT-Dienst und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTTwinMaker::SyncJob`

AWS Config -Regel: `iottwinmaker-sync-job-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS TwinMaker IoT-Synchronisierungsjob Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Synchronisierungsauftrag keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Synchronisierungsauftrag mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie

Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS TwinMaker IoT-Synchronisierungsjob finden Sie TagResourceim AWS IoT TwinMaker Benutzerhandbuch.

[IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-01.01, CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTTwinMaker::Workspace`

AWS Config -Regel: `iottwinmaker-workspace-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS TwinMaker IoT-Workspace Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn der Workspace keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Workspace mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS TwinMaker IoT-Arbeitsbereich finden Sie TagResourceim AWS IoT TwinMaker Benutzerhandbuch.

[IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTTwinMaker::Scene`

AWS Config -Regel: `iottwinmaker-scene-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS TwinMaker IoT-Szene Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn die Szene keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Szene mit keinem Schlüssel markiert ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS TwinMaker IoT-Szene finden Sie TagResourceim AWS IoT TwinMaker Benutzerhandbuch.

[IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTTwinMaker::Entity`

AWS Config -Regel: `iottwinmaker-entity-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS TwinMaker IoT-Entität Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredKeyTags`. Das Steuerelement schlägt fehl, wenn die Entität keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Entität mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS TwinMaker IoT-Entität finden Sie TagResourceim AWS IoT TwinMaker Benutzerhandbuch.

Security Hub CSPM-Steuerungen fürAWSIoT Wireless

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS IoT-Wireless-Service und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbarAWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::MulticastGroup`

AWS Config-Regel: `iotwireless-multicast-group-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS IoT Wireless Wireless-Multicast-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn die Multicast-Gruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Multicast-Gruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT-Wireless-Multicast-Gruppe finden Sie unter Taggen Ihrer AWS IoT Wireless Ressourcen im AWS IoT WirelessEntwicklerhandbuch.

[IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::ServiceProfile`

AWS Config-Regel: `iotwireless-service-profile-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS IoT Wireless Wireless-Dienstprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Dienstprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Dienstprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Wireless Wireless-Dienstprofil finden Sie unter Taggen Ihrer AWS IoT Wireless Ressourcen im AWS IoT WirelessEntwicklerhandbuch.

[IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::FuotaTask`

AWS Config-Regel: `iotwireless-fuota-task-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS IoT Wireless Firmware-Update Over-the-Air (FUOTA) über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredKeyTags` Die Steuerung schlägt fehl, wenn die FUOTA-Aufgabe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die FUOTA-Aufgabe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von

Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWSTagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Wireless FUOTA-Aufgabe finden Sie unter Tagging your AWS IoT Wireless resources im AWS IoT WirelessDeveloper Guide.

Security Hub CSPM-Steuerungen für Amazon IVS

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen des Amazon Interactive Video Service (IVS).

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IVS::PlaybackKeyPair`

AWS Config -Regel: `ivs-playback-key-pair-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon IVS-Wiedergabeschlüsselpaar Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn das Playback-Schlüsselpaar keine Tag-Tasten hat oder wenn es nicht alle im Parameter angegebenen Tasten hat`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Playback-Schlüsselpaar mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IVS-Wiedergabeschlüsselpaar finden Sie TagResourcein der Amazon IVS Real-Time Streaming API-Referenz.

[IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IVS::RecordingConfiguration`

AWS Config -Regel: `ivs-recording configuration-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon IVS-Aufzeichnungskonfiguration Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn die Aufzeichnungskonfiguration keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel enthält. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Aufzeichnungskonfiguration mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer IVS-Aufzeichnungskonfiguration finden Sie TagResourcein der Amazon Real-Time IVS-Streaming-API-Referenz.

[IVS.3] IVS-Kanäle sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IVS::Channel`

AWS Config -Regel: `ivs-channel-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon IVS-Kanal Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn der Kanal keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel hat. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Kanal mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IVS-Kanal finden Sie TagResourcein der Amazon IVS Real-Time Streaming API-Referenz.

Security Hub CSPM-Steuerelemente für Amazon Keyspaces

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Keyspaces.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Cassandra::Keyspace`

AWS Config -Regel: `cassandra-keyspace-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Keyspaces-Schlüsselraum Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredKeyTags` Die Steuerung schlägt fehl, wenn der Schlüsselraum keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Schlüsselraum mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon Keyspaces-Schlüsselraum finden Sie unter Hinzufügen von Tags zu einem Schlüsselraum im Amazon Keyspaces-Entwicklerhandbuch.

Security Hub CSPM-Steuerungen für Kinesis

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Kinesis.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::Kinesis::Stream`

AWS Config -Regel: kinesis-stream-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Kinesis Data Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt sind. Diese Steuerung schlägt fehl, wenn ein Kinesis-Stream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Server-side Verschlüsselung ist eine Funktion in Amazon Kinesis Data Streams, die Daten automatisch verschlüsselt, bevor sie sich im Ruhezustand befinden, und zwar mithilfe eines. AWS KMS key Die Daten werden verschlüsselt, bevor sie in die Speicherschicht des Kinesis-Streams geschrieben werden. Nach Abruf aus dem Speicher werden sie entschlüsselt. Daher werden Ihre Daten im Ruhezustand innerhalb des Amazon Kinesis Data Streams Streams-Service verschlüsselt.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Kinesis-Streams finden Sie unter Wie fange ich mit serverseitiger Verschlüsselung an? im Amazon Kinesis Developer Guide.

[Kinesis.2] Kinesis-Streams sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Kinesis::Stream`

AWS Config Regel: `tagged-kinesis-stream` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Kinesis Kinesis-Datenstream Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt

fehl, wenn der Datenstream keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Datenstrom mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Kinesis-Datenstream finden Sie unter Tagging your streams in Amazon Kinesis Data Streams im Amazon Kinesis Developer Guide.

[Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen

Schweregrad: Mittel

Ressourcentyp: `AWS::Kinesis::Stream`

AWS Config-Regel: kinesis-stream-backup-retention-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minimumBackupRetentionPeriod`	Mindestanzahl von Stunden, für die die Daten aufbewahrt werden sollen.	Zeichenfolge	24 bis 8760	168

Dieses Steuerelement prüft, ob ein Amazon Kinesis Kinesis-Datenstream eine Datenaufbewahrungsdauer hat, die größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn die Datenaufbewahrungsdauer den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Datenaufbewahrungsdauer angeben, verwendet Security Hub CSPM einen Standardwert von 168 Stunden.

In Kinesis Data Streams ist ein Datenstrom eine geordnete Abfolge von Datensätzen, in die in Echtzeit geschrieben und daraus gelesen werden soll. Datensätze werden vorübergehend in Shards in Ihrem Stream gespeichert. Der Zeitraum ab dem Hinzufügen eines Datensatzes bis zu dem Zeitpunkt, an dem er nicht mehr verfügbar ist, wird als Aufbewahrungszeitraum bezeichnet. Kinesis Data Streams macht Datensätze, die älter als die neue Aufbewahrungsfrist sind, fast sofort unzugänglich, nachdem die Aufbewahrungsfrist verkürzt wurde. Beispielsweise bedeutet eine Änderung des Aufbewahrungszeitraums von 24 Stunden auf 48 Stunden, dass Datensätze, die 23 Stunden und 55 Minuten vorher zum Stream hinzugefügt wurden, nach 24 Stunden weiterhin verfügbar sind.

Abhilfe

Informationen zum Ändern der Aufbewahrungsdauer von Backups für Ihre Kinesis Data Streams finden Sie unter Ändern der Datenaufbewahrungsdauer im Amazon Kinesis Data Streams Developer Guide.

Security Hub CSPM-Steuerungen für AWS KMS

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Key Management Service (AWS KMS) Dienst und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: iam-customer-policy-blocked-kms-actions

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(nicht anpassbar)
- `excludePermissionBoundaryPolicy`: `True` (nicht anpassbar)

Überprüft, ob die Standardversion der vom Kunden verwalteten IAM-Richtlinien es Prinzipalen erlaubt, die AWS KMS Entschlüsselungsaktionen für alle Ressourcen zu verwenden. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie. Darüber hinaus bewertet das Steuerelement sowohl angehängte als auch nicht verknüpfte, vom Kunden verwaltete Richtlinien. Inline-Richtlinien oder AWS verwaltete Richtlinien werden nicht geprüft.

Damit kontrollieren Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe

oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die `kms:ReEncryptFrom` Berechtigungen `kms:Decrypt` oder und nur die Schlüssel gewähren, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt Berechtigungen für alle Schlüssel zu gewähren, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie stattdessen `kms:Decrypt` nur Schlüssel in einer bestimmten Region für Ihr Konto. Durch die Anwendung des Prinzips der geringsten Rechte können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer vom Kunden verwalteten IAM-Richtlinie finden Sie unter Bearbeiten von kundenverwalteten Richtlinien im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, CRI Profile v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config -Regel: iam-inline-policy-blocked-kms-actions

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(nicht anpassbar)

Dieses Steuerelement prüft, ob die in Ihre IAM-Identitäten (Rolle, Benutzer oder Gruppe) eingebetteten Inline-Richtlinien die AWS KMS Entschlüsselung und erneute Verschlüsselung aller KMS-Schlüssel zulassen. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie.

Mit steuern Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die Berechtigungen gewähren, die sie benötigen, und nur für Schlüssel, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt die Erlaubnis für alle Schlüssel zu erteilen, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es den Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie die Erlaubnis stattdessen nur für bestimmte Schlüssel in einer bestimmten Region für Ihr Konto. Indem Sie das Prinzip der geringsten Rechte anwenden, können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer IAM-Inline-Richtlinie finden Sie unter Bearbeiten von Inline-Richtlinien im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

Verwandte Anforderungen: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), CRI Profile v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Kritisch

Art der Ressource: `AWS::KMS::Key`

AWS Config Regel: `kms-cmk-not-scheduled-for-deletion-2` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Löschung von KMS-Schlüsseln geplant ist. Die Steuerung schlägt fehl, wenn das Löschen eines KMS-Schlüssels geplant ist.

KMS-Schlüssel können nach dem Löschen nicht wiederhergestellt werden. Mit einem KMS-Schlüssel verschlüsselte Daten können auch dauerhaft nicht wiederhergestellt werden, wenn der KMS-Schlüssel gelöscht wird. Wenn aussagekräftige Daten unter einem KMS-Schlüssel verschlüsselt wurden, der gelöscht werden soll, sollten Sie erwägen, die Daten zu entschlüsseln oder die Daten erneut mit einem neuen KMS-Schlüssel zu verschlüsseln, sofern Sie nicht absichtlich eine kryptografische Löschung durchführen.

Wenn das Löschen eines KMS-Schlüssels geplant ist, wird eine obligatorische Wartezeit durchgesetzt, damit genügend Zeit zur Verfügung steht, um den Löschvorgang rückgängig zu machen, falls er versehentlich geplant wurde. Die standardmäßige Wartezeit beträgt 30 Tage, kann aber auf bis zu 7 Tage reduziert werden, wenn der KMS-Schlüssel gelöscht werden soll. Während der Wartezeit kann das geplante Löschen abgebrochen werden und der KMS-Schlüssel wird nicht gelöscht.

Weitere Informationen zum Löschen von KMS-Schlüsseln finden Sie unter Löschen von KMS-Schlüsseln im AWS Key Management Service Entwicklerhandbuch.

Abhilfe

Informationen zum Abbrechen einer geplanten Löschung von KMS-Schlüsseln finden Sie im AWS Key Management Service Entwicklerhandbuch unter So brechen Sie das Löschen von Schlüsseln ab (Konsole) unter So brechen Sie das Löschen von Schlüsseln ab.

[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.6, Benchmark v3.0 für CIS AWS Foundations. 0/3.6, Benchmark für CIS AWS Foundations v1.4. 0/3.8, Benchmark für CIS AWS Foundations v1.2. 0/2.8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-28 (3), PCI DSS v3.2. 1/36.6.4, PCI-DSS v4.0. 1/3.7.4, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::KMS::Key`

AWS Config -Regel: cmk-backing-key-rotation-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

AWS KMS ermöglicht Kunden die Rotation des Backing-Schlüssels, bei dem es sich um Schlüsselmaterial handelt, das im KMS-Schlüssel gespeichert ist AWS KMS und mit der Schlüssel-ID des KMS-Schlüssels verknüpft ist. Der Unterstützungsschlüssel wird zum Durchführen kryptografischer Vorgänge wie z. B. Ver- und Entschlüsselungen verwendet. Die automatische Schlüsselrotation speichert derzeit alle vorherigen Unterstützungsschlüssel, sodass eine transparente Entschlüsselung verschlüsselter Daten erfolgen kann.

CIS empfiehlt, die KMS-Schlüsselrotation zu aktivieren. Das Rotieren der Verschlüsselungsschlüssel trägt zur Verringerung der potenziellen Auswirkungen eines kompromittierten Schlüssels bei, da der Zugriff auf mit einem neuen Schlüssel verschlüsselte Daten mit einem vorherigen Schlüssel, der möglicherweise kompromittiert wurde, nicht möglich ist.

Abhilfe

Informationen zur Aktivierung der KMS-Schlüsselrotation finden Sie unter So aktivieren und deaktivieren Sie die automatische Schlüsselrotation im AWS Key Management Service Entwicklerhandbuch.

[KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::KMS::Key`

AWS Config -Regel: kms-key-policy-no-public-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dadurch wird geprüft, ob ein öffentlich zugänglich AWS KMS key ist. Die Steuerung schlägt fehl, wenn der KMS-Schlüssel öffentlich zugänglich ist.

Die Implementierung des Zugriffs mit den geringsten Rechten ist von grundlegender Bedeutung, um das Sicherheitsrisiko und die Auswirkungen von Fehlern oder böswilligen Absichten zu verringern. Wenn die Schlüsselrichtlinie für ein den Zugriff von externen Konten aus AWS KMS key zulässt, können Dritte möglicherweise Daten mithilfe des Schlüssels ver- und entschlüsseln. Dies könnte dazu führen, dass eine interne oder externe Bedrohung Daten aus dem System herausfiltert, AWS-Services das den Schlüssel verwendet.

> **Note**
>
> Dieses Steuerelement gibt auch ein `FAILED` Ergebnis zurück, AWS KMS key wenn Ihre Konfigurationen AWS Config verhindern, dass die Schlüsselrichtlinie im Konfigurationselement (CI) für den KMS-Schlüssel aufgezeichnet wird. Damit die Schlüsselrichtlinie im CI für AWS Config den KMS-Schlüssel aufgefüllt werden kann, muss die AWS Config Rolle Zugriff haben, um die Schlüsselrichtlinie mithilfe des GetKeyPolicyAPI-Aufrufs lesen zu können. Um diese Art von Problem zu behebenFAILED, überprüfen Sie die Richtlinien, die verhindern können, dass die AWS Config Rolle Lesezugriff auf die Schlüsselrichtlinie für den KMS-Schlüssel hat. Überprüfen Sie beispielsweise Folgendes:
>
> - Die Schlüsselrichtlinie für den KMS-Schlüssel.
> - Die darin enthaltenen Service Control Policies (SCPs) und Resource Control Policies (RCPs) gelten für Ihr Konto. AWS Organizations
> - Berechtigungen für die AWS Config Rolle, wenn Sie die AWS Config dienstbezogene Rolle nicht verwenden.

Darüber hinaus bewertet dieses Steuerelement keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Schlüsselrichtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Aktualisierung der wichtigsten Richtlinien für eine AWS KMS key finden Sie unter Wichtige Richtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Security Hub CSPM-Steuerungen für AWS Lambda

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Lambda Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, PCI DSS v4.0. 1/7.2.1, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: lambda-function-public-access-prohibited

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die ressourcenbasierte Richtlinie der Lambda-Funktion den öffentlichen Zugriff außerhalb Ihres Kontos verbietet. Die Kontrolle schlägt fehl, wenn der öffentliche Zugriff zulässig ist. Die Kontrolle schlägt auch fehl, wenn eine Lambda-Funktion von Amazon S3 aus aufgerufen wird und die Richtlinie keine Bedingung zur Beschränkung des öffentlichen Zugriffs enthält, z. B. `AWS:SourceAccount` Wir empfehlen, andere S3-Bedingungen zusammen mit `AWS:SourceAccount` in Ihrer Bucket-Richtlinie zu verwenden, um den Zugriff zu verfeinern.

> **Note**
>
> Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Richtlinie für die Lambda-Funktion nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

Die Lambda-Funktion sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihren Funktionscode ermöglichen kann.

Abhilfe

Um dieses Problem zu beheben, müssen Sie die ressourcenbasierte Richtlinie Ihrer Funktion aktualisieren, um Berechtigungen zu entfernen oder die Bedingung hinzuzufügen. `AWS:SourceAccount` Sie können die ressourcenbasierte Richtlinie nur über die Lambda-API oder aktualisieren. AWS CLI

Überprüfen Sie zunächst die ressourcenbasierte Richtlinie auf der Lambda-Konsole. Identifizieren Sie die Richtlinienaussage, deren `Principal` Feldwerte die Richtlinie öffentlich machen, z. B. oder. `"*"` `{ "AWS": "*" }`

Sie können die Richtlinie nicht von der Konsole aus bearbeiten. Um der Funktion Berechtigungen zu entziehen, führen Sie den remove-permissionBefehl von der aus AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

*<function-name>*Ersetzen Sie durch den Namen der Lambda-Funktion und *<statement-id>* durch die Anweisungs-ID (`Sid`) der Anweisung, die Sie entfernen möchten.

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/123.3.4, CRI-Profil v2. 2/PR. PS-02.01, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: lambda-function-settings-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `runtime`: `dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, java17.al2023, java11.al2023, java8.al2023, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3` (nicht anpassbar)

Dieses Steuerelement prüft, ob die Laufzeiteinstellungen der AWS Lambda Funktionen mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Die Steuerung schlägt fehl, wenn die Lambda-Funktion keine unterstützte Laufzeit verwendet, wie im Abschnitt Parameter angegeben. Security Hub CSPM ignoriert Funktionen mit dem Pakettyp. `Image`

Lambda-Laufzeiten basieren auf einer Kombination aus Betriebssystem, Programmiersprache und Softwarebibliotheken, die Wartungs- und Sicherheitsupdates unterliegen. Wenn eine Laufzeitkomponente für Sicherheitsupdates nicht mehr unterstützt wird, hat Lambda die Laufzeit als veraltet eingestuft. Auch wenn Sie keine Funktionen erstellen können, die die veraltete Runtime verwenden, ist die Funktion dennoch für die Verarbeitung von Aufrufereignissen verfügbar. Wir empfehlen sicherzustellen, dass Ihre Lambda-Funktionen aktuell sind und keine veralteten Laufzeitumgebungen verwenden. Eine Liste der unterstützten Laufzeiten finden Sie unter Lambda-Laufzeiten im AWS Lambda Developer Guide.

Abhilfe

Weitere Informationen zu unterstützten Laufzeiten und Zeitplänen für veraltete Versionen finden Sie unter Runtime Deprecation Policy im Developer Guide.AWS Lambda Wenn Sie Ihre Laufzeiten auf die neueste Version migrieren, folgen Sie der Syntax und Anleitung der Herausgeber der Sprache. Wir empfehlen außerdem, Runtime-Updates zu installieren, um das Risiko einer Beeinträchtigung Ihrer Workloads im seltenen Fall einer Runtime-Versionsinkompatibilität zu verringern.

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config Regel: lambda-inside-vpc

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Lambda-Funktion in einer Virtual Private Cloud (VPC) bereitgestellt ist. Die Steuerung schlägt fehl, wenn die Lambda-Funktion nicht in einer VPC bereitgestellt wird. Security Hub CSPM bewertet die Konfiguration des VPC-Subnetz-Routings nicht, um die öffentliche Erreichbarkeit zu ermitteln. Möglicherweise werden fehlgeschlagene Ergebnisse für Lambda @Edge -Ressourcen angezeigt.

Die Bereitstellung von Ressourcen in einer VPC verbessert die Sicherheit und Kontrolle über Netzwerkkonfigurationen. Solche Bereitstellungen bieten auch Skalierbarkeit und hohe Fehlertoleranz über mehrere Availability Zones hinweg. Sie können VPC-Bereitstellungen an unterschiedliche Anwendungsanforderungen anpassen.

Abhilfe

Informationen zur Konfiguration einer vorhandenen Funktion für die Verbindung zu privaten Subnetzen in Ihrer VPC finden Sie unter Konfiguration des VPC-Zugriffs im AWS Lambda Entwicklerhandbuch. Wir empfehlen, mindestens zwei private Subnetze für hohe Verfügbarkeit und mindestens eine Sicherheitsgruppe auszuwählen, die die Konnektivitätsanforderungen der Funktion erfüllt.

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: lambda-vpc-multi-az-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`availabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion, die eine Verbindung zu einer Virtual Private Cloud (VPC) herstellt, in mindestens der angegebenen Anzahl von Availability Zone (AZs) funktioniert. Die Steuerung schlägt fehl, wenn die Funktion nicht in mindestens der angegebenen Anzahl von AZs funktioniert. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub CSPM einen Standardwert von zwei AZs.

Die Bereitstellung von Ressourcen auf mehreren AZs ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur sicherzustellen. Verfügbarkeit ist eine zentrale Säule des dreifachen Sicherheitsmodells für Vertraulichkeit, Integrität und Verfügbarkeit. Alle Lambda-Funktionen, die eine Verbindung zu einer VPC herstellen, sollten über eine Multi-AZ-Bereitstellung verfügen, um sicherzustellen, dass eine einzelne Ausfallzone nicht zu einer vollständigen Betriebsunterbrechung führt.

Abhilfe

Wenn Sie Ihre Funktion so konfigurieren, dass sie eine Verbindung zu einer VPC in Ihrem Konto herstellt, geben Sie Subnetze in mehreren AZs an, um eine hohe Verfügbarkeit sicherzustellen. Anweisungen finden Sie unter Konfiguration des VPC-Zugriffs im AWS Lambda Entwicklerhandbuch.

Lambda führt automatisch andere Funktionen in mehreren AZs aus, um sicherzustellen, dass es für die Verarbeitung von Ereignissen im Falle einer Serviceunterbrechung in einer einzelnen Zone verfügbar ist.

[Lambda.6] Lambda-Funktionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config Regel: `tagged-lambda-function` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion über Tags mit den spezifischen Tasten verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Funktion keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Funktion mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Lambda-Funktion finden Sie unter Verwenden von Tags für Lambda-Funktionen im AWS Lambda Entwicklerhandbuch.

[Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CA-7, CRI Profile v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: lambda-function-xray-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das aktive Tracing mit für eine AWS Lambda Funktion aktiviert AWS X-Ray ist. Die Steuerung schlägt fehl, wenn die aktive Ablaufverfolgung mit für die Lambda-Funktion deaktiviert X-Ray ist.

AWS X-Ray kann AWS Lambda Funktionen zur Nachverfolgung und Überwachung bereitstellen, wodurch Zeit und Mühe beim Debuggen und Betrieb von Lambda-Funktionen eingespart werden können. Es kann Ihnen helfen, Fehler zu diagnostizieren und Leistungsengpässe, Verlangsamungen und Timeouts zu identifizieren, indem es die Latenz für Lambda-Funktionen aufschlüsselt. Es kann auch bei Datenschutz- und Compliance-Anforderungen helfen. Wenn Sie die aktive Ablaufverfolgung für eine Lambda-Funktion aktivieren, X-Ray erhalten Sie einen ganzheitlichen Überblick über den Datenfluss und die Verarbeitung innerhalb der Lambda-Funktion, sodass Sie potenzielle Sicherheitslücken oder nicht konforme Datenverarbeitungspraktiken identifizieren können. Diese Transparenz kann Ihnen helfen, die Integrität und Vertraulichkeit Ihrer Daten zu wahren und die Einhaltung der geltenden Vorschriften zu gewährleisten.

> **Note**
>
> AWS X-Ray Die Ablaufverfolgung wird derzeit nicht für Lambda-Funktionen mit Amazon Managed Streaming for Apache Kafka (Amazon MSK), selbstverwaltetem Apache Kafka,

Amazon MQ mit ActiveMQ und RabbitMQ oder Amazon DocumentDB DocumentDB-Ereignisquellenzuordnungen unterstützt.

Abhilfe

Informationen zur Aktivierung von Active Tracing für eine AWS Lambda Funktion finden Sie unter Visualize Lambda function invocations using AWS X-Ray im Developer Guide.AWS Lambda

Security Hub CSPM-Steuerungen für Macie

Diese AWS Security Hub CSPM Kontrollen bewerten den Amazon Macie-Service.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Macie.1] Amazon Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4, CRI Profile v2. 2/ID. AM-05.01, CRI-Profil v2. 2/ID. AM-05.02, CRI-Profil v2. 2/ID. AM-07.01, CRI-Profil v2. 2/PR. DS-01.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `macie-status-check`

Art des Zeitplans: Periodisch

Diese Kontrolle prüft, ob Amazon Macie für ein Konto aktiviert ist. Die Kontrolle schlägt fehl, wenn Macie für das Konto nicht aktiviert ist.

Amazon Macie erkennt sensible Daten mithilfe von maschinellem Lernen und Musterabgleich, bietet Einblick in Datensicherheitsrisiken und ermöglicht automatisierten Schutz vor diesen Risiken. Macie bewertet Ihre Amazon Simple Storage Service (Amazon S3) -Buckets automatisch und kontinuierlich im Hinblick auf Sicherheit und Zugriffskontrolle und generiert Ergebnisse, um Sie über potenzielle Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon S3-Daten zu informieren. Macie automatisiert auch die Erkennung und Meldung sensibler Daten, wie z. B. personenbezogener Daten

(PII), um Ihnen ein besseres Verständnis der Daten zu vermitteln, die Sie in Amazon S3 speichern. Weitere Informationen finden Sie im Amazon Macie Macie-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von Macie finden Sie unter Macie aktivieren im Amazon Macie Macie-Benutzerhandbuch.

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4, CRI-Profil v2. 2/PR. DS-01.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `macie-auto-sensitive-data-discovery-check`

Art des Zeitplans: Periodisch

Dieses Steuerelement prüft, ob die automatische Erkennung sensibler Daten für ein Amazon Macie-Administratorkonto aktiviert ist. Die Kontrolle schlägt fehl, wenn die automatische Erkennung sensibler Daten für ein Macie-Administratorkonto nicht aktiviert ist. Dieses Steuerelement gilt nur für Administratorkonten.

Macie automatisiert die Erkennung und Meldung sensibler Daten, wie z. B. persönlich identifizierbare Informationen (PII), in Amazon Simple Storage Service (Amazon S3) -Buckets. Mit der automatisierten Erkennung sensibler Daten bewertet Macie kontinuierlich Ihr Bucket-Inventar und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie analysiert dann die ausgewählten Objekte und untersucht sie auf sensible Daten. Im Verlauf der Analysen aktualisiert Macie Statistiken, Inventardaten und andere Informationen, die Macie zu Ihren S3-Daten bereitstellt. Macie generiert auch Ergebnisse, um gefundene sensible Daten zu melden.

Abhilfe

Informationen zum Erstellen und Konfigurieren automatisierter Discovery-Jobs für sensible Daten zur Analyse von Objekten in S3-Buckets finden Sie unter Konfiguration der automatisierten Erkennung sensibler Daten für Ihr Konto im Amazon Macie Macie-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon MSK

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Managed Streaming for Apache Kafka (Amazon MSK). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4,, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: msk-in-cluster-node-require-tls

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon MSK-Cluster bei der Übertragung mit HTTPS (TLS) zwischen den Broker-Knoten des Clusters verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Klartext-Kommunikation für eine Cluster-Broker-Knotenverbindung aktiviert ist.

HTTPS bietet eine zusätzliche Sicherheitsebene, da TLS für die Übertragung von Daten verwendet wird. Damit kann verhindert werden, dass potenzielle Angreifer mithilfe von Person-in-the-Middle-Angriffen oder ähnlichen Angriffen den Netzwerkverkehr belauschen oder manipulieren. Standardmäßig verschlüsselt Amazon MSK Daten bei der Übertragung mit TLS. Sie können diese Standardeinstellung jedoch bei der Erstellung des Clusters überschreiben. Wir empfehlen die Verwendung verschlüsselter Verbindungen über HTTPS (TLS) für Broker-Knotenverbindungen.

Abhilfe

Informationen zur Aktualisierung der Verschlüsselungseinstellungen für einen Amazon MSK-Cluster finden Sie unter Aktualisieren der Sicherheitseinstellungen eines Clusters im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. IR-04.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: msk-enhanced-monitoring-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon MSK-Cluster eine erweiterte Überwachung konfiguriert ist, die durch eine Überwachungsebene von mindestens `PER_TOPIC_PER_BROKER` angegeben wird. Die Steuerung schlägt fehl, wenn die Überwachungsebene für den Cluster auf `DEFAULT` oder `PER_BROKER` gesetzt ist.

Die `PER_TOPIC_PER_BROKER` Überwachungsebene bietet detailliertere Einblicke in die Leistung Ihres MSK-Clusters und bietet auch Metriken zur Ressourcennutzung, z. B. zur CPU- und Speicherauslastung. Auf diese Weise können Sie Leistungsengpässe und Ressourcennutzungsmuster für einzelne Themen und Broker identifizieren. Diese Transparenz kann wiederum die Leistung Ihrer Kafka-Broker optimieren.

Abhilfe

Gehen Sie wie folgt vor, um die erweiterte Überwachung für einen MSK-Cluster zu konfigurieren:

1. Öffnen Sie die Amazon MSK-Konsole unter? https://console.aws.amazon.com/msk/home region=us-east-1#/home/.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie dann einen Cluster aus.
3. Wählen Sie für Aktion die Option Überwachung bearbeiten aus.
4. Wählen Sie die Option für Erweiterte Überwachung auf Themenebene aus.
5. Wählen Sie Änderungen speichern aus.

Weitere Informationen zu Überwachungsebenen finden Sie unter Amazon MSK-Metriken für die Überwachung von Standard-Brokern mit CloudWatch im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::KafkaConnect::Connector`

AWS Config Regel: `msk-connect-connector-encrypted` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon MSK Connect-Konnektor während der Übertragung verschlüsselt ist. Diese Kontrolle schlägt fehl, wenn der Connector bei der Übertragung nicht verschlüsselt wird.

Daten während der Übertragung beziehen sich auf Daten, die von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Sie können die Verschlüsselung bei der Übertragung aktivieren, wenn Sie einen MSK Connect-Connector erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Connectors nicht ändern. Weitere Informationen finden Sie unter Create a Connector im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: msk-cluster-public-access-disabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der öffentliche Zugriff für einen Amazon MSK-Cluster deaktiviert ist. Die Kontrolle schlägt fehl, wenn der öffentliche Zugriff für den MSK-Cluster aktiviert ist.

Standardmäßig können Clients nur dann auf einen Amazon MSK-Cluster zugreifen, wenn sie sich in derselben VPC wie der Cluster befinden. Die gesamte Kommunikation zwischen Kafka-Clients und einem MSK-Cluster ist standardmäßig privat und Streaming-Daten werden nicht über das Internet übertragen. Wenn ein MSK-Cluster jedoch so konfiguriert ist, dass er öffentlichen Zugriff zulässt, kann jeder im Internet eine Verbindung zu Apache Kafka-Brokern herstellen, die innerhalb des Clusters ausgeführt werden. Dies kann zu Problemen wie unberechtigtem Zugriff, Datenschutzverletzungen oder der Ausnutzung von Sicherheitslücken führen. Wenn Sie den Zugriff auf einen Cluster einschränken, indem Sie Authentifizierungs- und Autorisierungsmaßnahmen vorschreiben, können Sie dazu beitragen, vertrauliche Informationen zu schützen und die Integrität Ihrer Ressourcen aufrechtzuerhalten.

Abhilfe

Informationen zur Verwaltung des öffentlichen Zugriffs auf einen Amazon MSK-Cluster finden Sie unter Aktivieren des öffentlichen Zugriffs auf einen von MSK bereitgestellten Cluster im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::KafkaConnect::Connector`

AWS Config -Regel: msk-connect-connector-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für einen Amazon MSK-Connector aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für den MSK-Connector deaktiviert ist.

Amazon MSK-Konnektoren integrieren externe Systeme und Amazon-Services mit Apache Kafka, indem sie kontinuierlich Streaming-Daten aus einer Datenquelle in einen Apache Kafka-Cluster oder kontinuierlich Daten aus einem Cluster in eine Datensenke kopieren. MSK Connect kann Protokollereignisse schreiben, die beim Debuggen eines Connectors helfen können. Wenn Sie einen Connector erstellen, können Sie null oder mehr der folgenden Protokollziele angeben: Amazon CloudWatch Logs, Amazon S3 und Amazon Data Firehose.

> **Note**
>
> Vertrauliche Konfigurationswerte können in Konnektor-Protokollen erscheinen, wenn ein Plugin diese Werte nicht als Secret definiert. Kafka Connect behandelt undefinierte Konfigurationswerte genauso wie jeden anderen Klartext-Wert.

Abhilfe

Um die Protokollierung für einen vorhandenen Amazon MSK-Connector zu aktivieren, müssen Sie den Connector mit der entsprechenden Protokollierungskonfiguration neu erstellen. Informationen zu Konfigurationsoptionen finden Sie unter Logging for MSK Connect im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: msk-unrestricted-access-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob der nicht authentifizierte Zugriff für einen Amazon MSK-Cluster aktiviert ist. Die Kontrolle schlägt fehl, wenn der nicht authentifizierte Zugriff für den MSK-Cluster aktiviert ist.

Amazon MSK unterstützt Client-Authentifizierungs- und Autorisierungsmechanismen, um den Zugriff auf einen Cluster zu kontrollieren. Diese Mechanismen überprüfen die Identität der Clients, die sich mit dem Cluster verbinden, und bestimmen, welche Aktionen Clients ausführen können. Ein MSK-Cluster kann so konfiguriert werden, dass er nicht authentifizierten Zugriff ermöglicht, sodass jeder Client mit Netzwerkkonnektivität Kafka-Themen veröffentlichen und abonnieren kann, ohne Anmeldeinformationen angeben zu müssen. Das Ausführen eines MSK-Clusters ohne Authentifizierung verstößt gegen das Prinzip der geringsten Rechte und kann den Cluster unberechtigtem Zugriff aussetzen. Es kann jedem Client ermöglichen, auf Daten in Kafka-Themen zuzugreifen, diese zu ändern oder zu löschen, was möglicherweise zu Datenschutzverletzungen, unbefugten Datenänderungen oder Dienstunterbrechungen führen kann. Wir empfehlen, Authentifizierungsmechanismen wie IAM-Authentifizierung oder Mutual TLS zu aktivieren SASL/SCRAM, um eine angemessene Zugriffskontrolle zu gewährleisten und die Einhaltung der Sicherheitsbestimmungen zu gewährleisten.

Abhilfe

Informationen zum Ändern der Authentifizierungseinstellungen für einen Amazon MSK-Cluster finden Sie in den folgenden Abschnitten des Amazon Managed Streaming for Apache Kafka Developer Guide: Sicherheitseinstellungen eines Amazon MSK-Clusters aktualisieren und Authentifizierung und Autorisierung für Apache Kafka-APIs.

Security Hub CSPM-Steuerelemente für Amazon MQ

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon MQ. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AU-2,, NIST.800-53.r5 AU-3 NIST.800-53.r5 AU-12 NIST.800-53.r5 SI-4, PCI DSS v4.0. 1/103.3.3, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-cloudwatch-audit-log-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon MQ ActiveMQ-Broker Auditprotokolle an Amazon Logs streamt. CloudWatch Die Kontrolle schlägt fehl, wenn der Broker keine Auditprotokolle in Logs streamt. CloudWatch

Durch die Veröffentlichung von CloudWatch ActiveMQ-Broker-Protokollen in Logs können Sie CloudWatch Alarme und Metriken erstellen, die die Sichtbarkeit sicherheitsrelevanter Informationen erhöhen.

Abhilfe

Informationen zum Streamen von CloudWatch ActiveMQ-Broker-Protokollen in Logs finden Sie unter Konfiguration von Amazon MQ für ActiveMQ-Protokolle im Amazon MQ Developer Guide.

[MQ.4] Amazon MQ-Broker sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config Regel: `tagged-amazonmq-broker` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon MQ-Broker über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Broker keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter `requiredTagKeys` angegebenen Schlüssel verfügt. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Broker mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon MQ-Broker finden Sie unter Tagging resources im Amazon MQ Developer Guide.

[MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-active-deployment-mode`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ ActiveMQ-Broker auf eingestellt ist. active/standby Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Active/standby Die Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ ActiveMQ-Broker in einem. AWS-Region Der active/standby Bereitstellungsmodus umfasst zwei Broker-Instances in zwei verschiedenen Availability Zones, die in einem redundanten Paar konfiguriert sind. Diese Broker kommunizieren synchron mit Ihrer Anwendung, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen ActiveMQ-Brokers mit active/standby Bereitstellungsmodus finden Sie unter Erstellen und Konfigurieren eines ActiveMQ-Brokers im Amazon MQ Developer Guide. Wählen Sie für den Bereitstellungsmodus Broker. Active/standby Sie können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

[MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-rabbit-deployment-mode`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ RabbitMQ-Broker auf Cluster-Bereitstellung eingestellt ist. Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Die Cluster-Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ RabbitMQ-Broker in einem. AWS-Region Die Cluster-Bereitstellung ist eine logische Gruppierung von drei RabbitMQ-Broker-Knoten, von denen jeder über ein eigenes Amazon Elastic Block Store (Amazon EBS) -Volume und einen gemeinsamen Status verfügt. Die Cluster-Bereitstellung stellt sicher, dass Daten auf alle Knoten im Cluster repliziert werden, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen RabbitMQ-Brokers mit Cluster-Bereitstellungsmodus finden Sie unter Erstellen und Herstellen einer Verbindung zu einem RabbitMQ-Broker im Amazon MQ Developer Guide. Wählen Sie für den Bereitstellungsmodus die Option Cluster-Bereitstellung. Sie

können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

Security Hub CSPM-Steuerungen für Neptune

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Neptune.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer Neptune-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die Verschlüsselung von Produktionsdateisystemen im Ruhezustand.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Neptune-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht

ändern. Weitere Informationen finden Sie unter Encrypting Neptune resources at rest im Neptune-Benutzerhandbuch.

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7(8), PCI DSS v4.0. 1/103.3.3, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-cloudwatch-log-export-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Neptune-DB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch `EnableCloudWatchLogsExport`sollte auf eingestellt sein. `Audit`

Amazon Neptune und Amazon CloudWatch sind integriert, sodass Sie Leistungskennzahlen sammeln und analysieren können. Neptune sendet automatisch Messwerte an Alarme CloudWatch und unterstützt CloudWatch diese auch. Audit-Logs sind hochgradig anpassbar. Wenn Sie eine Datenbank prüfen, kann jeder Vorgang an den Daten überwacht und in einem Audit-Trail protokolliert werden, einschließlich Informationen darüber, auf welchen Datenbankcluster zugegriffen wird und wie. Wir empfehlen, diese Protokolle an zu senden, CloudWatch um Ihnen bei der Überwachung Ihrer Neptune-DB-Cluster zu helfen.

Abhilfe

Informationen zum Veröffentlichen von Neptune-Audit-Logs in CloudWatch Logs finden Sie unter Neptune-Logs in Amazon CloudWatch Logs veröffentlichen im Neptune-Benutzerhandbuch. Wählen Sie im Abschnitt Protokollexporte die Option Audit aus.

[Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config -Regel: `neptune-cluster-snapshot-public-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist. Die Steuerung schlägt fehl, wenn ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist.

Ein manueller Snapshot eines Neptune-DB-Clusters sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-KontenÖffentliche Schnappschüsse können zu einer unbeabsichtigten Offenlegung von Daten führen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Neptune-DB-Cluster-Snapshots finden Sie unter Freigeben eines DB-Cluster-Snapshots im Neptune-Benutzerhandbuch.

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CM-3, CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen Neptune-DB-Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet eine zusätzliche Schutzebene vor dem versehentlichen Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Neptune-DB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Neptune-DB-Cluster finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora Aurora-Benutzerhandbuch.

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02, CRI-Profil v2. 2/RC. RP-03.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-backup-retention-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`minimumBackupRetentionPeriod`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster automatische Backups aktiviert sind und ob die Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn Backups für den Neptune-DB-Cluster nicht aktiviert sind oder wenn die Aufbewahrungszeit kürzer als der angegebene Zeitrahmen ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub CSPM einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich nach einem Sicherheitsvorfall schneller zu erholen und die Widerstandsfähigkeit Ihrer Systeme zu stärken. Durch die Automatisierung von Backups für Ihre Neptune-DB-Cluster können Sie Ihre Systeme bis zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren.

Abhilfe

Informationen zur Aktivierung automatisierter Backups und zur Festlegung einer Aufbewahrungsfrist für Backups für Ihre Neptune-DB-Cluster finden Sie unter Automatisierte Backups aktivieren im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Aufbewahrungszeitraum für Backup einen Wert größer oder gleich 7.

[Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (18), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config -Regel: `neptune-cluster-snapshot-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster-Snapshot im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Sie können einen vorhandenen Neptune-DB-Cluster-Snapshot nicht verschlüsseln. Stattdessen müssen Sie den Snapshot in einem neuen DB-Cluster wiederherstellen und die Verschlüsselung auf dem Cluster aktivieren. Sie können einen verschlüsselten Snapshot aus dem verschlüsselten Cluster erstellen. Anweisungen finden Sie unter Wiederherstellung aus einem DB-Cluster-Snapshot und Erstellen eines DB-Cluster-Snapshots in Neptune im Neptune-Benutzerhandbuch.

[Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. PS-06.10

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-iam-database-authentication`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Datenbankauthentifizierung für einen Neptune-DB-Cluster nicht aktiviert ist.

Die IAM-Datenbankauthentifizierung für Amazon Neptune Neptune-Datenbankcluster macht das Speichern von Benutzeranmeldeinformationen in der Datenbankkonfiguration überflüssig, da die Authentifizierung extern mithilfe von IAM verwaltet wird. Wenn die IAM-Datenbankauthentifizierung aktiviert ist, muss jede Anfrage mit Signature Version 4 signiert werden. AWS

Abhilfe

Standardmäßig ist die IAM-Datenbankauthentifizierung deaktiviert, wenn Sie einen Neptune-DB-Cluster erstellen. Informationen zur Aktivierung finden Sie unter Aktivieren der IAM-Datenbankauthentifizierung in Neptune im Neptune-Benutzerhandbuch.

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01, CRI-Profil v2. 2/ID. AM-08.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-copy-tags-to-snapshot-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster so konfiguriert ist, dass er alle Tags in Snapshots kopiert, wenn die Snapshots erstellt werden. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster nicht so konfiguriert ist, dass er Tags in Snapshots kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie sollten Snapshots auf die gleiche Weise kennzeichnen wie ihre übergeordneten Amazon RDS-Datenbankcluster. Durch das Kopieren von Tags wird sichergestellt, dass die Metadaten für die DB-Snapshots mit denen der übergeordneten Datenbankcluster übereinstimmen und dass die Zugriffsrichtlinien für den DB-Snapshot auch mit denen der übergeordneten DB-Instance übereinstimmen.

Abhilfe

Informationen zum Kopieren von Tags in Snapshots für Neptune-DB-Cluster finden Sie unter Kopieren von Tags in Neptune im Neptune-Benutzerhandbuch.

[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-multi-az-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Neptune Neptune-DB-Cluster über Read-Replica-Instances in mehreren Availability Zones (AZs) verfügt. Die Steuerung schlägt fehl, wenn der Cluster nur in einer AZ bereitgestellt wird.

Wenn eine AZ nicht verfügbar ist und während regelmäßiger Wartungsereignisse, dienen Read-Replicas als Failover-Ziele für die primäre Instanz. Wenn die primäre Instance ausfällt, stuft Neptune eine Read-Replica-Instance zur primären Instance herauf. Wenn Ihr DB-Cluster dagegen keine Read-Replica-Instances enthält, bleibt Ihr DB-Cluster auch dann nicht verfügbar, wenn die primäre Instance ausfällt, bis sie neu erstellt wurde. Re-creating Die primäre Instance dauert erheblich länger als das Heraufstufen einer Read-Replica. Um eine hohe Verfügbarkeit zu gewährleisten, empfehlen wir, eine

oder mehrere Read-Replica-Instances zu erstellen, die dieselbe DB-Instance-Klasse wie die primäre Instance haben und sich in anderen AZs als die primäre Instance befinden.

Abhilfe

Informationen zur Bereitstellung eines Neptune-DB-Clusters in mehreren AZs finden Sie unter Read-replica DB-Instances in einem Neptune-DB-Cluster im Neptune-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS Network Firewall

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Network Firewall Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: netfw-multi-az-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet, ob eine über mehrere Availability Zones (AZs) verwaltete Firewall eingesetzt AWS Network Firewall wird. Die Steuerung schlägt fehl, wenn eine Firewall nur in einer AZ bereitgestellt wird.

AWS Die globale Infrastruktur umfasst mehrere AWS-Regionen. AZs sind physisch getrennte, isolierte Standorte innerhalb jeder Region, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Durch die Bereitstellung einer Netzwerk-Firewall-

Firewall auf mehreren AZs können Sie den Verkehr zwischen AZs verteilen und verlagern, was Ihnen bei der Entwicklung hochverfügbarer Lösungen hilft.

Abhilfe

Bereitstellung einer Netzwerk-Firewall-Firewall auf mehreren AZs

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus.
3. Wählen Sie auf der Seite Firewalls die Firewall aus, die Sie bearbeiten möchten.
4. Wählen Sie auf der Seite mit den Firewall-Details die Registerkarte Firewall-Details aus.
5. Wählen Sie im Abschnitt Zugeordnete Richtlinie und VPC die Option Bearbeiten aus.
6. Um eine neue AZ hinzuzufügen, wählen Sie Neues Subnetz hinzufügen. Wählen Sie die AZ und das Subnetz aus, die Sie verwenden möchten. Stellen Sie sicher, dass Sie mindestens zwei AZs auswählen.
7. Wählen Sie Speichern.

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, (3) NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (7), NIST.800-53.r5 AU-9 (9), (8) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config -Regel: netfw-logging-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS Network Firewall Firewall aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für mindestens einen Protokolltyp nicht aktiviert ist oder wenn das Protokollierungsziel nicht existiert.

Mithilfe der Protokollierung können Sie die Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Firewalls aufrechterhalten. In der Network Firewall bietet Ihnen die Protokollierung detaillierte Informationen über den Netzwerkverkehr, einschließlich der Uhrzeit, zu der die Stateful-Engine einen Paketfluss empfangen hat, detaillierte Informationen über den Paketfluss und alle statusbehafteten Regelaktionen, die gegen den Paketfluss ergriffen wurden.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Firewall finden Sie unter Aktualisieren der Protokollierungskonfiguration einer Firewall im AWS Network Firewall Entwicklerhandbuch.

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.1, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: netfw-policy-rule-group-associated

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob einer Netzwerk-Firewall-Richtlinie statusbehaftete oder statuslose Regelgruppen zugeordnet sind. Die Steuerung schlägt fehl, wenn keine statusfreien oder statusbehafteten Regelgruppen zugewiesen werden.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon Virtual Private Cloud (Amazon VPC) überwacht und verarbeitet. Die Konfiguration von statusfreien und statusbehafteten Regelgruppen hilft beim Filtern von Paketen und Datenströmen und definiert die standardmäßige Verarbeitung des Datenverkehrs.

Abhilfe

Informationen zum Hinzufügen einer Regelgruppe zu einer Netzwerk-Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Informationen zum Erstellen und Verwalten von Regelgruppen finden Sie unter Regelgruppen in AWS Network Firewall.

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. IR-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: netfw-policy-default-action-full-packets

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die standardmäßige statuslose Aktion für vollständige Pakete für eine Netzwerkfirewall-Richtlinie Drop oder Forward ist. Die Steuerung ist erfolgreich, wenn `Drop` oder ausgewählt `Forward` ist, und schlägt fehl, wenn sie ausgewählt `Pass` ist.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Die Standardeinstellung `Pass` kann unbeabsichtigten Datenverkehr zulassen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Wählen Sie für Standardaktionen

ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1),, NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, 3.13.6, CRI Profile v2. NIST.800-171.r2 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. IR-01.03

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: netfw-policy-default-action-fragment-packets

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die standardmäßige statuslose Aktion für fragmentierte Pakete für eine Netzwerkfirewall-Richtlinie Drop oder Forward ist. Die Steuerung ist erfolgreich, wenn `Drop` oder ausgewählt `Forward` ist, und schlägt fehl, wenn sie ausgewählt `Pass` ist.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Die Standardeinstellung `Pass` kann unbeabsichtigten Datenverkehr zulassen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Wählen Sie für Standardaktionen ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, 3.13.6, CRI Profile v2. NIST.800-171.r2 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-01.05

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::RuleGroup`

AWS Config -Regel: netfw-stateless-rule-group-not-empty

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine statuslose Regelgruppe Regeln AWS Network Firewall enthält. Das Steuerelement schlägt fehl, wenn die Regelgruppe keine Regeln enthält.

Eine Regelgruppe enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeitet. Eine leere statuslose Regelgruppe kann, wenn sie in einer Firewallrichtlinie vorhanden ist, den Eindruck erwecken, dass die Regelgruppe den Datenverkehr verarbeitet. Wenn die statuslose Regelgruppe jedoch leer ist, verarbeitet sie keinen Datenverkehr.

Abhilfe

Informationen zum Hinzufügen von Regeln zu Ihrer Netzwerk-Firewall-Regelgruppe finden Sie unter Aktualisieren einer statusbehafteten Regelgruppe im AWS Network Firewall Entwicklerhandbuch. Wählen Sie auf der Seite mit den Firewall-Details für Stateless Rule Group die Option Bearbeiten aus, um Regeln hinzuzufügen.

[NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config Regel: `tagged-networkfirewall-firewall` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Firewall keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Firewall mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Firewall finden Sie unter Tagging AWS Network Firewall resources im AWS Network Firewall Developer Guide.

[NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config Regel: `tagged-networkfirewall-firewallpolicy` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall-Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Firewall-Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Firewall-Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Richtlinie finden Sie unter Tagging AWS Network Firewall resources im AWS Network Firewall Developer Guide.

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), CRI Profile v2. 2/PR. IR-01.02

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: netfw-deletion-protection-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS Network Firewall Firewall der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz für eine Firewall nicht aktiviert ist.

AWS Network Firewall ist ein zustandsorientierter, verwalteter Dienst für Netzwerk-Firewall und Erkennung von Eindringlingen, mit dem Sie den Datenverkehr zu, von oder zwischen Ihren Virtual Private Clouds (VPCs) überprüfen und filtern können. Die Löschschutzeinstellung schützt vor versehentlichem Löschen der Firewall.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine bestehende Netzwerk-Firewall-Firewall finden Sie unter Aktualisieren einer Firewall im AWS Network Firewall Entwicklerhandbuch. Wählen Sie unter Änderungsschutz die Option Aktivieren aus. Sie können den Löschschutz auch aktivieren, indem Sie die UpdateFirewallDeleteProtectionAPI aufrufen und das `DeleteProtection` Feld auf setzen. `true`

[NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CM-3, CRI Profile v2. 2/DE. CM-09.03, CRI-Profil v2.

2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: netfw-subnet-change-protection-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Subnetz-Änderungsschutz für eine AWS Network Firewall Firewall aktiviert ist. Die Steuerung schlägt fehl, wenn der Subnetzänderungsschutz für die Firewall nicht aktiviert ist.

AWS Network Firewall ist ein zustandsorientierter, verwalteter Dienst zur Netzwerk-Firewall und zur Erkennung von Eindringlingen, mit dem Sie den Datenverkehr zu, von oder zwischen Ihren Virtual Private Clouds (VPCs) untersuchen und filtern können. Wenn Sie den Subnetzänderungsschutz für eine Netzwerkfirewall-Firewall aktivieren, können Sie die Firewall vor versehentlichen Änderungen an den Subnetzzuordnungen der Firewall schützen.

Abhilfe

Informationen zur Aktivierung des Subnetzänderungsschutzes für eine bestehende Netzwerkfirewall-Firewall finden Sie unter Aktualisieren einer Firewall im AWS Network Firewall Entwicklerhandbuch.

Security Hub CSPM-Steuerungen für Amazon Service OpenSearch

Diese AWS Security Hub CSPM Kontrollen bewerten den OpenSearch Service und die Ressourcen von Amazon OpenSearch Service (Service). Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5

SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-encrypted-at-rest`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, AWS KMS werden Ihre Verschlüsselungsschlüssel gespeichert und verwaltet. AWS KMS Verwendet für die Verschlüsselung den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln ()AES-256.

Weitere Informationen zur OpenSearch Service-Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende OpenSearch Domains finden Sie unter Enabling encryption of data at rest im Amazon OpenSearch Service Developer Guide.

[Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11)

NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-in-vpc-only`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen.

Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. Weitere Resource-based Informationen finden Sie im Amazon OpenSearch Service Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. Bewährte Sicherheitsmethoden für Ihre VPC finden Sie im Amazon VPC-Benutzerhandbuch.

OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerksteuerungen, um den Zugriff auf OpenSearch Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen. Security Hub empfiehlt, öffentliche OpenSearch Domains zu VPCs zu migrieren, um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder eine andere Domäne erstellen oder dieses Steuerelement deaktivieren.

Anweisungen finden Sie unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC im Amazon OpenSearch Service Developer Guide.

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-node-to-node-encryption-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in OpenSearch Domänen die Verschlüsselung von Knoten zu Knoten aktiviert ist. Diese Steuerung schlägt fehl, wenn die Knoten-zu-Knoten-Verschlüsselung in der Domäne deaktiviert ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit Person-in-the-Middle- oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der Knoten-zu-Knoten-Verschlüsselung für OpenSearch Domänen wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zum Aktivieren der Knoten-zu-Knoten-Verschlüsselung auf einer OpenSearch Domain finden Sie unter Enabling Node-to-Knoten-Verschlüsselung im Amazon Service Developer Guide. OpenSearch

[Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `logtype = 'error'`(nicht anpassbar)

Dieses Steuerelement prüft, ob OpenSearch Domänen so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden. Dieses Steuerelement schlägt fehl, wenn die Fehlerprotokollierung für eine Domäne nicht aktiviert CloudWatch ist.

Sie sollten Fehlerprotokolle für OpenSearch Domänen aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Bearbeitung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zum Aktivieren der Protokollveröffentlichung finden Sie unter Aktivieren der Protokollveröffentlichung (Konsole) im Amazon OpenSearch Service Developer Guide.

[Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), PCI DSS

v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-audit-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar) — Security Hub CSPM füllt diesen Parameter nicht aus. Comma-separated Liste der CloudWatch Log-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

Dieses Steuerelement prüft, ob für OpenSearch Domänen die Auditprotokollierung aktiviert ist. Dieses Steuerelement schlägt fehl, wenn für eine OpenSearch Domäne die Überwachungsprotokollierung nicht aktiviert ist.

Auditprotokolle sind in hohem Maße anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren OpenSearch Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener AuthentifizierungenOpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Anweisungen zur Aktivierung von Audit-Logs finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service Developer Guide.

[Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-data-node-fault-tolerance`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob OpenSearch Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist`true`. Dieses Steuerelement schlägt für eine OpenSearch Domäne fehl, wenn sie `instanceCount` weniger als 3 `zoneAwarenessEnabled` ist oder ist`false`.

Um eine hohe Verfügbarkeit und Fehlertoleranz auf Clusterebene zu erreichen, sollte eine OpenSearch Domäne über mindestens drei Datenknoten verfügen. Durch die Bereitstellung einer OpenSearch Domäne mit mindestens drei Datenknoten wird der Clusterbetrieb gewährleistet, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer OpenSearch Domäne zu ändern

1. Melden Sie sich bei der AWS Konsole an und öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.
2. Wählen Sie unter Meine Domains den Namen der Domain aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus.
3. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl größer als ein`3`. Wenn Sie in drei Availability Zones bereitstellen, legen Sie die Zahl auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.
4. Wählen Sie Absenden aus.

Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Schützen > Secure Access Management > Eingeschränkte sensible API-Aktionen

Schweregrad: Hoch

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-access-control-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen eine differenzierte Zugriffskontrolle aktiviert ist. Die Steuerung schlägt fehl, wenn die feinkörnige Zugriffskontrolle nicht aktiviert ist. Fine-grained Die Zugriffskontrolle erfordert`advanced-security-options`, dass der OpenSearch Parameter `update-domain-config` aktiviert ist.

Fine-grained Die Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten bei Amazon OpenSearch Service zu kontrollieren.

Abhilfe

Informationen zur Aktivierung einer detaillierten Zugriffskontrolle finden Sie unter Fine-grained Zugriffskontrolle in Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. IR-01.05, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-https-required`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(nicht anpassbar)

Diese Steuerung prüft, ob ein Amazon OpenSearch Service-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Kontrolle schlägt fehl, wenn der OpenSearch Domain-Endpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert ist oder wenn HTTPS nicht aktiviert ist.

HTTPS (TLS) kann verwendet werden, um potenzielle Angreifer daran zu hindern, Person-in-the-Middle- oder ähnliche Angriffe zu nutzen, um den Netzwerkverkehr abzuhören oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Verwenden Sie den UpdateDomainConfigAPI-Vorgang, um die TLS-Verschlüsselung zu aktivieren. Konfigurieren Sie das DomainEndpointOptionsFeld, um den Wert für anzugebenTLSSecurityPolicy. Weitere Informationen finden Sie unter Node-to-node Verschlüsselung im Amazon OpenSearch Service Developer Guide.

[Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config Regel: `tagged-opensearch-domain` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon OpenSearch Service-Domain Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer OpenSearch Service-Domain finden Sie unter Arbeiten mit Tags im Amazon OpenSearch Service Developer Guide.

Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-update-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob auf einer Amazon OpenSearch Service-Domain das neueste Softwareupdate installiert ist. Die Kontrolle schlägt fehl, wenn ein Softwareupdate verfügbar, aber nicht für die Domain installiert ist.

OpenSearch Service-Softwareupdates bieten die neuesten Plattformkorrekturen, Updates und Funktionen, die für die Umgebung verfügbar sind. Wenn Sie bei der Installation von Patches auf dem neuesten Stand bleiben, können Sie die Sicherheit und Verfügbarkeit der Domain aufrechterhalten. Wenn bei den erforderlichen Updates keine Maßnahmen ergriffen werden, wird die Service-Software automatisch aktualisiert (in der Regel nach 2 Wochen). Wir empfehlen, Updates in Zeiten mit geringem Datenverkehr auf der Domain zu planen, um Betriebsunterbrechungen zu minimieren.

Abhilfe

Informationen zur Installation von Softwareupdates für eine OpenSearch Domain finden Sie unter Ein Update starten im Amazon OpenSearch Service Developer Guide.

[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36 NIST.800-53.r5 SI-13, CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-primary-node-fault-tolerance`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon OpenSearch Service-Domain mit mindestens drei dedizierten Primärknoten konfiguriert ist. Die Kontrolle schlägt fehl, wenn die Domain weniger als drei dedizierte Primärknoten hat.

OpenSearch Der Dienst verwendet dedizierte Primärknoten, um die Clusterstabilität zu erhöhen. Ein dedizierter primärer Knoten führt Clusterverwaltungsaufgaben aus, speichert jedoch keine Daten und reagiert auch nicht auf Anfragen zum Hochladen von Daten. Wir empfehlen die Verwendung von Multi-AZ mit Standby, wodurch jeder OpenSearch Produktionsdomäne drei dedizierte Primärknoten hinzugefügt werden.

Abhilfe

Informationen zum Ändern der Anzahl der Primärknoten für eine OpenSearch Domain finden Sie unter Erstellen und Verwalten von Amazon OpenSearch Service-Domains im Amazon OpenSearch Service Developer Guide.

Security Hub CSPM-Steuerungen für AWS Private CA

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Private Certificate Authority (AWS Private CA) Dienst und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. PS-01.07

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::ACMPCA::CertificateAuthority`

AWS Config -Regel: `acm-pca-root-ca-disabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob es AWS Private CA eine deaktivierte Stammzertifizierungsstelle (CA) gibt. Die Steuerung schlägt fehl, wenn die Stammzertifizierungsstelle aktiviert ist.

Mit AWS Private CA können Sie eine Zertifizierungsstellenhierarchie erstellen, die eine Stammzertifizierungsstelle und untergeordnete Zertifizierungsstellen umfasst. Sie sollten die Verwendung der Stammzertifizierungsstelle für tägliche Aufgaben minimieren, insbesondere in Produktionsumgebungen. Die Stammzertifizierungsstelle sollte nur zur Ausstellung von Zertifikaten für zwischengeschaltete Zertifizierungsstellen verwendet werden. Dadurch kann die Stammzertifizierungsstelle gespeichert werden, ohne Schaden zu nehmen, während die Zwischenzertifizierungsstellen das tägliche Ausstellen von Endentitätszertifikaten übernehmen.

Abhilfe

Informationen zum Deaktivieren der Root-CA finden Sie unter CA-Status aktualisieren im AWS Private Certificate Authority Benutzerhandbuch.

[PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ACMPCA::CertificateAuthority`

AWS Config -Regel: `acmpca-certificate-authority-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS private Zertifizierungsstelle über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Die Kontrolle schlägt fehl, wenn die Zertifizierungsstelle keine Tagschlüssel hat oder wenn sie nicht über alle im Parameter angegebenen Schlüssel verfügt`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Zertifizierungsstelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter Bewährte Methoden und Strategien im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer AWS privaten Zertifizierungsstelle finden Sie unter Hinzufügen von Stichwörtern für Ihre private Zertifizierungsstelle im AWS Private Certificate Authority Benutzerhandbuch.

Security Hub CSPM-Steuerungen für Amazon RDS

Diese AWS Security Hub CSPM Kontrollen bewerten die Ressourcen von Amazon Relational Database Service (Amazon RDS) und Amazon RDS. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[RDS.1] Der RDS-Snapshot sollte privat sein

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Ressourcentyp:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config -Regel: `rds-snapshots-public-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Snapshots öffentlich sind. Die Steuerung schlägt fehl, wenn RDS-Snapshots öffentlich sind. Dieses Steuerelement bewertet RDS-Instances, Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster.

RDS-Snapshots werden verwendet, um die Daten auf Ihren RDS-Instances zu einem bestimmten Zeitpunkt zu sichern. Sie können verwendet werden, um frühere Zustände von RDS-Instances wiederherzustellen.

Ein RDS-Snapshot darf nur öffentlich sein, wenn dies beabsichtigt ist. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, wird der Snapshot dadurch für alle verfügbar. AWS-Konten Dies kann zu einer unbeabsichtigten Offenlegung von Daten Ihrer RDS-Instance führen.

Beachten Sie, dass die AWS Config Regel die Änderung möglicherweise bis zu 12 Stunden lang nicht erkennen kann, wenn die Konfiguration so geändert wird, dass sie öffentlich zugänglich ist. Bis die AWS Config Regel die Änderung erkennt, ist die Prüfung erfolgreich, obwohl die Konfiguration gegen die Regel verstößt.

Weitere Informationen zum Teilen eines DB-Snapshots finden Sie unter Freigeben eines DB-Snapshots im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-Snapshots finden Sie unter Einen Snapshot teilen im Amazon RDS-Benutzerhandbuch. Für die Sichtbarkeit von DB-Snapshots wählen wir Privat.

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/22.2.3, Benchmark v3.0 für CIS AWS Foundations. 0/2.3.3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), PCI DSS v3.2. 1/13.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-public-access-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Instances öffentlich zugänglich sind, indem es das `PubliclyAccessible` Feld im Instance-Konfigurationselement auswertet.

Der `PubliclyAccessible`-Wert in der RDS-Instance-Konfiguration gibt an, ob die DB-Instance öffentlich zugänglich ist. Wenn die DB-Instance mit konfiguriert ist`PubliclyAccessible`, handelt es sich um eine Internet-facing Instance mit einem öffentlich auflösbaren DNS-Namen, der in eine öffentliche IP-Adresse aufgelöst wird. Wenn die DB-Instance nicht öffentlich zugänglich ist, handelt es sich um eine interne Instance mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird.

Sofern Sie nicht beabsichtigen, dass Ihre RDS-Instance öffentlich zugänglich ist, sollte die RDS-Instance nicht mit `PubliclyAccessible` Value konfiguriert werden. Dadurch könnte unnötiger Datenverkehr zu Ihrer Datenbank-Instance entstehen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-DB-Instances finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für öffentlichen Zugriff die Option Nein.

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/22.2.1, Benchmark v3.0 für CIS AWS Foundations. 0/23.3.1, Benchmark für CIS AWS Foundations v1.4. 0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-storage-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Speicherverschlüsselung für Ihre Amazon RDS-DB-Instances aktiviert ist.

Diese Steuerung ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Um eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in RDS-DB-Instances zu erhalten, sollten Sie Ihre RDS-DB-Instances so konfigurieren, dass sie im Ruhezustand verschlüsselt werden. Um Ihre RDS-DB-Instances und Snapshots im Ruhezustand zu verschlüsseln, aktivieren Sie die Verschlüsselungsoption für Ihre RDS-DB-Instances. Daten, die im Ruhezustand verschlüsselt werden, umfassen den zugehörigen Speicherplatz für DB-Instances, deren automatisierte Backups, Read Replicas und Snapshots.

RDS-verschlüsselte DB-Instances verwenden den offenen AES-256 Standard-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre RDS-DB-Instances hostet. Nachdem Ihre Daten verschlüsselt wurden, verarbeitet Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um die Verschlüsselung anzuwenden.

Die Amazon RDS-Verschlüsselung ist derzeit für alle Datenbank-Engines und Speichertypen verfügbar. Amazon-RDS-Verschlüsselung ist für die meisten DB-Instance-Klassen verfügbar. Informationen zu DB-Instance-Klassen, die die Amazon RDS-Verschlüsselung nicht unterstützen, finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zur Verschlüsselung von DB-Instances in Amazon RDS finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Ressourcentyp:, `AWS::RDS::DBClusterSnapshot` `AWS::RDS::DBSnapshot`

AWS Config -Regel: `rds-snapshot-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Snapshot verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Snapshot nicht verschlüsselt ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Snapshots von Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Clustern generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. Daten in RDS-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zum Verschlüsseln eines RDS-Snapshots finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch. Wenn Sie eine RDS-DB-Instance verschlüsseln, umfassen die verschlüsselten Daten den der Instance zugrunde liegenden Speicher, ihre automatisierten Backups, Read Replicas und Snapshots.

Sie können eine RDS-DB-Instance nur verschlüsseln, wenn Sie sie erstellen, nicht nachdem die DB-Instance erstellt wurde. Da es jedoch möglich ist, die Kopie eines unverschlüsselten Snapshots zu verschlüsseln, können Sie quasi eine Verschlüsselung zu einer unverschlüsselten DB-Instance hinzufügen. Dies lässt sich durchführen, indem Sie einen Snapshot von Ihrer DB-Instance erstellen

und dann eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie Ihre DB-Instance aus dem verschlüsselten Snapshot wiederherstellen und verfügen so über eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance.

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/2.2.4, NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-multi-az-support`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Instances aktiviert ist. Die Steuerung schlägt fehl, wenn eine RDS-DB-Instance nicht mit mehreren Availability Zones (AZs) konfiguriert ist. Diese Steuerung gilt nicht für RDS-DB-Instances, die Teil einer Multi-AZ DB-Cluster-Bereitstellung sind.

Die Konfiguration von Amazon RDS-DB-Instances mit AZs trägt dazu bei, die Verfügbarkeit der gespeicherten Daten sicherzustellen. Multi-AZ Bereitstellungen ermöglichen einen automatisierten Failover bei Problemen mit der AZ-Verfügbarkeit und während der regulären RDS-Wartung.

Abhilfe

Um Ihre DB-Instances in mehreren AZs bereitzustellen, finden Sie unter Ändern einer DB-Instance zu einer Multi-AZ DB-Instance-Bereitstellung im Amazon RDS-Benutzerhandbuch.

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. IR-04.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-enhanced-monitoring-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`monitoringInterval`	Anzahl der Sekunden zwischen den Erfassungsintervallen von Überwachungsmetriken	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Kein Standardwert

Dieses Steuerelement prüft, ob die erweiterte Überwachung für eine Amazon Relational Database Service (Amazon RDS) -DB-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn die erweiterte Überwachung für die Instance nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `monitoringInterval` Parameter angeben, ist die Steuerung nur erfolgreich, wenn die Metriken zur erweiterten Überwachung für die Instance im angegebenen Intervall erfasst werden.

In Amazon RDS ermöglicht Enhanced Monitoring eine schnellere Reaktion auf Leistungsänderungen in der zugrunde liegenden Infrastruktur. Diese Leistungsänderungen können zu einer mangelnden Verfügbarkeit der Daten führen. Enhanced Monitoring bietet Echtzeit-Metriken des Betriebssystems, auf dem Ihre RDS-DB-Instance läuft. Auf der Instance ist ein Agent installiert. Der Agent kann Metriken genauer abrufen, als dies auf der Hypervisor-Ebene möglich ist.

Metriken von Enhanced Monitoring sind nützlich, um zu sehen, wie unterschiedliche Prozesse oder Threads auf einer DB-Instance die CPU nutzen. Weitere Informationen finden Sie unter Enhanced Monitoring (Erweiterte Überwachung) im Amazon-RDS-Benutzerhandbuch.

Abhilfe

Detaillierte Anweisungen zur Aktivierung von Enhanced Monitoring für Ihre DB-Instance finden Sie unter Enhanced Monitoring einrichten und aktivieren im Amazon RDS-Benutzerhandbuch.

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), CRI Profile v2. 2/PR. IR-03.01

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen RDS-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen RDS-DB-Cluster kein Löschschutz aktiviert ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Die Aktivierung des Cluster-Löschschutzes bietet zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch eine nicht autorisierte Entität.

Wenn der Löschschutz aktiviert ist, kann ein RDS-Cluster nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen RDS-DB-Cluster finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (nicht anpassbar)

Dieses Steuerelement prüft, ob für Ihre RDS-DB-Instances, die eine der aufgelisteten Datenbank-Engines verwenden, der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für eine RDS-DB-Instance kein Löschschutz aktiviert ist.

Die Aktivierung des Schutzes vor dem Löschen von Instances ist eine zusätzliche Schutzebene gegen das versehentliche Löschen von Datenbanken oder das Löschen durch eine nicht autorisierte Entität.

Solange der Löschschutz aktiviert ist, kann eine RDS-DB-Instance nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.9] RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (10), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. IR-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance so konfiguriert ist, dass sie die folgenden Protokolle in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn die Instance nicht so konfiguriert ist, dass sie die folgenden CloudWatch Protokolle in Logs veröffentlicht:

- Oracle: Alert, Audit, Trace, Listener
- PostgreSQL: Postgresql, Aktualisierung
- MySQL: Audit, Fehler, Allgemein, SlowQuery
- MariaDB: Audit, Fehler, Allgemein, SlowQuery
- SQL Server: Fehler, Agent
- Aurora-MySQL: Prüfung, Fehler, Allgemein, SlowQuery
- Aurora-PostgreSQL: Postgresql

Für RDS-Datenbanken sollten die entsprechenden Protokolle aktiviert sein. Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen der an RDS gestellten Anfragen. Datenbankprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Abhilfe

Informationen zum Veröffentlichen von RDS-Datenbankprotokollen in CloudWatch Logs finden Sie unter Spezifizieren der in CloudWatch Logs zu veröffentlichenden Logs im Amazon RDS-Benutzerhandbuch.

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-iam-authentication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine RDS-DB-Instance die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Authentifizierung nicht für RDS-DB-Instances konfiguriert ist. Diese Steuerung bewertet nur RDS-Instances mit den folgenden Engine-Typen:`mysql`,`postgres`,, `aurora` `aurora-mysql`aurora-postgresql, und. `mariadb` Eine RDS-Instanz muss sich außerdem in einem der folgenden Zustände befinden, damit ein Ergebnis generiert werden kann:`available`, `backing-up`storage-optimization, oder`storage-full`.

Die IAM-Datenbankauthentifizierung ermöglicht die Authentifizierung von Datenbank-Instances mit einem Authentifizierungstoken anstelle eines Kennworts. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Datenbankauthentifizierung auf einer RDS-DB-Instance finden Sie unter Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung im Amazon RDS-Benutzerhandbuch.

[RDS.11] Für RDS-Instances sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBInstance`

AWS Config -Regel: `db-instance-backup-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`backupRetentionMinimum`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	
`checkReadReplicas`	Überprüft, ob für RDS-DB-Instances Backups für Read Replicas aktiviert sind	Boolesch	Nicht anpassbar	`false`	

Diese Kontrolle prüft, ob für eine Amazon Relational Database Service Service-Instance automatische Backups aktiviert sind und ob eine Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Read Replicas sind von der Evaluierung ausgeschlossen. Die Kontrolle schlägt fehl, wenn Backups für die Instanz nicht aktiviert sind oder wenn die Aufbewahrungsdauer unter dem angegebenen Zeitraum liegt. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub CSPM einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich schneller nach einem Sicherheitsvorfall zu erholen, und stärken die Widerstandsfähigkeit Ihrer Systeme. Mit Amazon RDS können Sie tägliche Snapshots des gesamten Instance-Volumes konfigurieren. Weitere Informationen zu automatisierten Amazon RDS-Backups finden Sie unter Arbeiten mit Backups im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren automatisierter Backups auf einer RDS-DB-Instance finden Sie unter Automatisierte Backups aktivieren im Amazon RDS-Benutzerhandbuch.

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-iam-authentication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon RDS-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist.

Die IAM-Datenbankauthentifizierung ermöglicht eine passwortlose Authentifizierung bei Datenbank-Instances. Die Authentifizierung verwendet ein Authentifizierungstoken. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Authentifizierung für einen DB-Cluster finden Sie unter Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/22.2.2, Benchmark für CIS AWS Foundations v3.0. 0/2.3.2, NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-automatic-minor-version-upgrade-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für eine Amazon RDS-DB-Instance automatische Upgrades für Nebenversionen aktiviert sind. Die Kontrolle schlägt fehl, wenn automatische Upgrades für Nebenversionen für die RDS-DB-Instance nicht aktiviert sind.

> **Note**
>
> Diese Steuerung bewertet jede Amazon RDS-DB-Instance unabhängig. Für Amazon Aurora Aurora-Cluster erfordern automatische Upgrades kleinerer Versionen, dass Sie diese Einstellung auf dem Cluster aktivieren. Sie müssen diese Einstellung auch für alle Instances im Cluster aktivieren. Ein `PASSED` Ergebnis für eine einzelne Instanz garantiert nicht, dass Upgrades durchgeführt werden, wenn Sie die Einstellung nicht auch auf Clusterebene aktiviert haben.
>
> Diese Steuerung berücksichtigt auch nicht Konfigurationen, die automatische Upgrades von Nebenversionen nicht unterstützen. Dazu gehören Aurora-Cluster in einer globalen Aurora-Datenbank und Aurora-MySQL-Cluster mit regionsübergreifenden Read Replicas. Bei diesen Konfigurationen führt die Steuerung möglicherweise zu Bewertungsergebnissen, die das tatsächliche Upgrade-Verhalten nicht genau widerspiegeln.

Durch automatische Upgrades kleinerer Versionen wird eine Datenbank regelmäßig auf die neuesten Versionen der Datenbank-Engine aktualisiert. Das Upgrade beinhaltet jedoch möglicherweise nicht immer die aktuelle Datenbank-Engine-Version. Wenn Sie Ihre Datenbanken zu bestimmten Zeiten auf bestimmten Versionen belassen müssen, empfehlen wir Ihnen, ein manuelles Upgrade auf die Datenbankversionen durchzuführen, die Sie gemäß Ihrem erforderlichen Zeitplan benötigen. Bei kritischen Sicherheitsproblemen oder wenn für eine Version das Ende des Supports erreicht ist, führt Amazon RDS möglicherweise ein Upgrade für eine kleinere Version durch, auch wenn Sie die Option Automatisches Upgrade der Nebenversion nicht aktiviert haben. Weitere Informationen finden Sie in der Amazon RDS-Upgrade-Dokumentation für Ihre spezifische Datenbank-Engine:

- Automatische Nebenversions-Upgrades für RDS for MariaDB
- Automatische Upgrades kleinerer Versionen für RDS for MySQL

- Automatische Upgrades kleinerer Versionen für RDS for PostgreSQL
- Versionen von Db2 auf Amazon RDS
- Upgrades kleinerer Oracle-Versionen
- Upgrades der Microsoft SQL Server-DB-Engine

Abhilfe

Informationen zur Aktivierung automatischer Unterversions-Upgrades für eine bestehende DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für das automatische Upgrade der Nebenversion Ja aus.

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/GV. OC-05.04, CRI-Profil v2. 2/ID. IM-02.06, CRI-Profil v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: `aurora-mysql-backtracking-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`BacktrackWindowInHours`	Anzahl der Stunden für die Rückverfolgung eines Aurora MySQL-Clusters	Double	`0.1` auf `72`	Kein Standardwert	

Dieses Steuerelement prüft, ob für einen Amazon Aurora Aurora-Cluster Backtracking aktiviert ist. Die Steuerung schlägt fehl, wenn für den Cluster kein Backtracking aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `BacktrackWindowInHours` Parameter angeben, ist die Steuerung nur erfolgreich, wenn der Cluster für den angegebenen Zeitraum zurückverfolgt wird.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Aurora-Backtracking reduziert die Zeit für die Wiederherstellung einer Datenbank auf einen bestimmten Zeitpunkt. Dazu ist keine Datenbankwiederherstellung erforderlich.

Abhilfe

Informationen zur Aktivierung von Aurora-Backtracking finden Sie unter Backtracking konfigurieren im Amazon Aurora Aurora-Benutzerhandbuch.

Beachten Sie, dass Sie Backtracking nicht auf einem vorhandenen Cluster aktivieren können. Stattdessen können Sie einen Clone erstellen, für den Backtracking aktiviert ist. Weitere Informationen zu den Einschränkungen von Aurora-Backtracking finden Sie in der Liste der Einschränkungen unter Backtracking im Überblick.

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/2.2.4, NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-multi-az-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Cluster aktiviert ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster nicht in mehreren Availability Zones (AZs) bereitgestellt wird.

RDS-DB-Cluster sollten für mehrere AZs konfiguriert werden, um die Verfügbarkeit der gespeicherten Daten sicherzustellen. Die Bereitstellung auf mehreren AZs ermöglicht einen automatisierten Failover im Falle eines AZ-Verfügbarkeitsproblems und während regelmäßiger RDS-Wartungsereignisse.

Abhilfe

Um Ihre DB-Cluster in mehreren AZs bereitzustellen, finden Sie unter Ändern einer DB-Instance zu einer Multi-AZ DB-Instance-Bereitstellung im Amazon RDS-Benutzerhandbuch.

Die Schritte zur Behebung sind für globale Aurora-Datenbanken unterschiedlich. Um mehrere Availability Zones für eine globale Aurora-Datenbank zu konfigurieren, wählen Sie Ihren DB-Cluster aus. Wählen Sie dann Aktionen und Leser hinzufügen und geben Sie mehrere AZs an. Weitere Informationen finden Sie unter Hinzufügen von Aurora Replicas zu einem DB-Cluster im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/ID. AM-08.01, CRI-Profil v2. 2/ID. AM-08.03

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: `rds-cluster-copy-tags-to-snapshots-enabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Aurora Aurora-DB-Cluster so konfiguriert ist, dass Tags automatisch in Snapshots des DB-Clusters kopiert werden, wenn die Snapshots erstellt werden. Die Steuerung schlägt fehl, wenn der Aurora-DB-Cluster nicht so konfiguriert ist, dass Tags bei der Erstellung der Snapshots automatisch in Snapshots des Clusters kopiert werden.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre Amazon Aurora Aurora-DB-Cluster, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Aurora-DB-Snapshots sollten dieselben Tags wie ihre übergeordneten DB-Cluster haben. In Amazon Aurora können Sie einen DB-Cluster so konfigurieren,

dass automatisch alle Tags für den Cluster in Snapshots des Clusters kopiert werden. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass DB-Snapshots dieselben Tags erben wie ihre übergeordneten DB-Cluster.

Abhilfe

Informationen zur Konfiguration eines Amazon Aurora Aurora-DB-Clusters für das automatische Kopieren von Tags in DB-Snapshots finden Sie unter Ändern eines Amazon Aurora Aurora-DB-Clusters im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI-Profil v2. 2/ID. AM-08.01, CRI-Profil v2. 2/ID. AM-08.03

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `rds-instance-copy-tags-to-snapshots-enabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RDS-DB-Instances so konfiguriert sind, dass sie bei der Erstellung der Snapshots alle Tags in Snapshots kopieren.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre RDS-DB-Instances, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Snapshots sollten auf die gleiche Weise gekennzeichnet werden wie ihre übergeordneten RDS-Datenbank-Instances. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass Snapshots die Tags ihrer übergeordneten Datenbank-Instances erben.

Abhilfe

Informationen zum automatischen Kopieren von Tags in Snapshots für eine RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie Tags in Snapshots kopieren aus.

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-cluster-event-notifications-configured` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbankcluster Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelle und Ereigniskategorie aktiviert sind:

```
DBCluster: ["maintenance","failure"]
```

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwendet Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Cluster-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Cluster
Zu berücksichtigende Cluster	Alle Cluster
Zu berücksichtigende Veranstaltungskategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-instance-event-notifications-configured` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbank-Instances Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelltyp und Ereigniskategorie aktiviert sind:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen

finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Instances
Instances, die aufgenommen werden sollen	Alle Instanzen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-pg-event-notifications-configured` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist. Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

```
DBParameterGroup: ["configuration change"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von Ereignisbenachrichtigungen für RDS-Datenbankparametergruppen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Parametergruppen
Zu berücksichtigende Parametergruppen	Alle Parametergruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-sg-event-notifications-configured` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist. Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Sicherheitsgruppen
Zu berücksichtigende Sicherheitsgruppen	Alle Sicherheitsgruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `rds-no-default-ports` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-Cluster oder eine RDS-Instanz einen anderen Port als den Standardport der Datenbank-Engine verwendet. Die Steuerung schlägt fehl, wenn der RDS-Cluster oder die RDS-Instanz den Standardport verwendet. Diese Steuerung gilt nicht für RDS-Instances, die Teil eines Clusters sind.

Wenn Sie einen bekannten Port verwenden, um einen RDS-Cluster oder eine RDS-Instanz bereitzustellen, kann ein Angreifer Informationen über den Cluster oder die Instanz erraten. Der Angreifer kann diese Informationen in Verbindung mit anderen Informationen verwenden, um eine Verbindung zu einem RDS-Cluster oder einer RDS-Instance herzustellen oder zusätzliche Informationen über Ihre Anwendung zu erhalten.

Wenn Sie den Port ändern, müssen Sie auch die vorhandenen Verbindungszeichenfolgen aktualisieren, die für die Verbindung mit dem alten Port verwendet wurden. Sie sollten auch die Sicherheitsgruppe der DB-Instance überprüfen, um sicherzustellen, dass sie eine Eingangsregel enthält, die Konnektivität auf dem neuen Port ermöglicht.

Abhilfe

Informationen zum Ändern des Standardports einer vorhandenen RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Informationen zum Ändern des Standardports eines vorhandenen RDS-DB-Clusters finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora Aurora-Benutzerhandbuch. Ändern Sie für den Datenbankport den Portwert auf einen Wert, der nicht dem Standard entspricht.

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-default-admin-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Datenbank-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB). Diese Regel schlägt fehl, wenn der Admin-Benutzername auf den Standardwert gesetzt ist.

Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Erstellung der RDS-Datenbank geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Um den Admin-Benutzernamen zu ändern, der mit dem Amazon RDS-Datenbank-Cluster verknüpft ist, erstellen Sie einen neuen RDS-Datenbank-Cluster und ändern Sie den Standard-Admin-Benutzernamen beim Erstellen der Datenbank.

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2, CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-default-admin-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Sie den Administrator-Benutzernamen für Amazon Relational Database Service (Amazon RDS) -Datenbank-Instances gegenüber dem Standardwert geändert haben. Die Steuerung schlägt fehl, wenn der Administrator-Benutzername auf den Standardwert gesetzt ist. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB) und für RDS-Instances, die Teil eines Clusters sind.

Standardmäßige Administratorbenutzernamen in Amazon RDS-Datenbanken sind allgemein bekannt. Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern, um das Risiko eines unbeabsichtigten Zugriffs zu verringern.

Abhilfe

Um den mit einer RDS-Datenbank-Instance verknüpften Administrator-Benutzernamen zu ändern, erstellen Sie zunächst eine neue RDS-Datenbank-Instance. Ändern Sie den standardmäßigen Administratorbenutzernamen beim Erstellen der Datenbank.

[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

Kategorie: Wiederherstellen > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/RC. RP-01.01

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: **`rds-resources-protected-by-backup-plan`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`backupVaultLockCheck`	Das Steuerelement gibt einen `PASSED` Befund aus, wenn der Parameter auf true gesetzt ist und	Boolesch	`true` oder `false`	Kein Standardwert	

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	die Ressource AWS Backup Vault Lock verwendet.			

Diese Kontrolle bewertet, ob Amazon RDS-DB-Instances durch einen Backup-Plan abgedeckt sind. Diese Kontrolle schlägt fehl, wenn die RDS-DB-Instance nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, wird die Kontrolle nur erfolgreich ausgeführt, wenn die Instance in einem AWS Backup gesperrten Tresor gesichert ist.

> **Note**
>
> Dieses Steuerelement wertet Neptune- und DocumentDB-Instanzen nicht aus. Es bewertet auch keine RDS-DB-Instances, die Mitglieder eines Clusters sind.

AWS Backup ist ein vollständig verwalteter Backup-Service, der die gesamte Datensicherung zentralisiert und automatisiert. AWS-Services Mit können Sie Backup-Richtlinien erstellen AWS Backup, die als Backup-Pläne bezeichnet werden. Mit diesen Plänen können Sie Ihre Sicherungsanforderungen definieren, z. B. wie häufig Ihre Daten gesichert werden sollen und wie lange diese Sicherungen aufbewahrt werden sollen. Durch die Aufnahme von RDS-DB-Instances in einen Backup-Plan können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer RDS-DB-Instance zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-cluster-encrypted-at-rest`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer RDS-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die Verschlüsselung von Produktionsdateisystemen im Ruhezustand.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen RDS-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter Verschlüsseln eines Amazon Aurora Aurora-DB-Clusters im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.28] RDS-DB-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: `tagged-rds-dbcluster` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.29] Snapshots von RDS-DB-Clustern sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config Regel: `tagged-rds-dbclustersnapshot` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster-Snapshot finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.30] RDS-DB-Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `tagged-rds-dbinstance` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die DB-Instance mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Instance finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSecurityGroup`

AWS Config Regel: `tagged-rds-dbsecuritygroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Sicherheitsgruppe finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.32] RDS-DB-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSnapshot`

AWS Config Regel: `tagged-rds-dbsnapshot` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Snapshot finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSubnetGroup`

AWS Config Regel: `tagged-rds-dbsubnetgroups` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die DB-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Subnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Subnetzgruppe finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-aurora-mysql-audit-logging-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon Aurora MySQL-DB-Cluster so konfiguriert ist, dass er Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn der Cluster nicht für die Veröffentlichung von Audit-Logs in Logs konfiguriert ist. CloudWatch Das Steuerelement generiert keine Ergebnisse für Aurora Serverless v1-DB-Cluster.

In Audit-Protokollen werden Datenbankaktivitäten aufgezeichnet, einschließlich Anmeldeversuchen, Datenänderungen, Schemaänderungen und anderen Ereignissen, die aus Sicherheits- und Compliance-Gründen geprüft werden können. Wenn Sie einen Aurora MySQL-DB-Cluster so konfigurieren, dass er Audit-Logs in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht, können Sie eine Echtzeitanalyse der Protokolldaten durchführen. CloudWatch Logs speichert Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigen CloudWatch.

> **Note**
>
> Eine alternative Möglichkeit, Audit-Logs in Logs zu CloudWatch veröffentlichen, besteht darin, die erweiterte Überwachung zu aktivieren und den DB-Parameter `server_audit_logs_upload` auf Clusterebene auf zu setzen. `1` Die Standardeinstellung für ist`server_audit_logs_upload parameter`. `0` Wir empfehlen jedoch, stattdessen die folgenden Anweisungen zur Problembehebung zu verwenden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Veröffentlichen von Aurora CloudWatch MySQL-DB-Cluster-Prüfprotokollen in Logs finden Sie unter Veröffentlichen von Amazon Aurora CloudWatch Aurora-MySQL-Protokollen in Amazon Logs im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-cluster-auto-minor-version-upgrade-enable`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob das automatische Upgrade einer Nebenversion für einen Amazon RDS-DB-Cluster, einschließlich Aurora-DB-Cluster, aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für den DB-Cluster nicht aktiviert ist.

Mit dem automatischen Upgrade der Nebenversion können Sie Ihren DB-Cluster auf dem neuesten Stand halten. Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung des automatischen Upgrades für Nebenversionen auf RDS-Datenbankclustern erhält der Cluster zusammen mit den Instances im Cluster automatische Updates für die Nebenversion, sobald neue Versionen verfügbar sind. Die Updates werden während des Wartungsfensters automatisch angewendet.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades für Nebenversionen auf Multi-AZ DB-Clustern finden Sie unter Ändern eines Multi-AZ DB-Clusters im Amazon RDS-Benutzerhandbuch.

Informationen zur Aktivierung des automatischen Upgrades auf Aurora-DB-Clustern finden Sie unter Ändern eines Amazon Aurora Aurora-DB-Clusters im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-postgresql-logs-to-cloudwatch

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`logTypes`	Comma-separated Liste der Protokolltypen, die in Logs veröffentlicht werden sollen CloudWatch	StringList	Nicht anpassbar	`postgresql`

Dieses Steuerelement prüft, ob eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn die PostgreSQL-DB-Instance nicht so konfiguriert ist, dass sie die im `logTypes` Parameter genannten Protokolltypen in Logs veröffentlicht. CloudWatch

Die Datenbankprotokollierung liefert detaillierte Aufzeichnungen von Anfragen, die an eine RDS-Instance gestellt wurden. PostgreSQL generiert Ereignisprotokolle, die nützliche Informationen für Administratoren enthalten. Durch die Veröffentlichung dieser CloudWatch Protokolle in Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert die Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigenCloudWatch.

Abhilfe

Informationen zum Veröffentlichen von PostgreSQL-DB-Instance-Protokollen in CloudWatch Logs finden Sie unter Veröffentlichen von PostgreSQL-Protokollen in Amazon CloudWatch Logs im Amazon RDS-Benutzerhandbuch.

[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: rds-aurora-postgresql-logs-to-cloudwatch

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Aurora PostgreSQL-DB-Cluster für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn der Aurora PostgreSQL-DB-Cluster nicht für die Veröffentlichung von PostgreSQL-Protokollen in Logs konfiguriert ist. CloudWatch

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an einen RDS-Cluster gestellt wurden. Aurora PostgreSQL generiert Ereignisprotokolle, die nützliche Informationen für Administratoren enthalten. Durch die Veröffentlichung dieser CloudWatch Protokolle in Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert die Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigen CloudWatch.

Abhilfe

Informationen zum Veröffentlichen von Aurora CloudWatch PostgreSQL-DB-Cluster-Protokollen in Logs finden Sie unter Veröffentlichen von Aurora PostgreSQL-Protokollen in Amazon CloudWatch Logs im Amazon RDS-Benutzerhandbuch.

[RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-postgres-instance-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for PostgreSQL Datenbank-Instance (DB) während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.force_ssl` Parameter für die der Instance zugeordnete Parametergruppe auf `0` (aus) gesetzt ist. Dieses Steuerelement bewertet keine RDS-DB-Instances, die Teil eines DB-Clusters sind.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen dazu, dass alle Verbindungen zu Ihrer RDS for PostgreSQL-DB-Instance SSL verwenden müssen, finden Sie unter Verwenden von SSL mit einer PostgreSQL-DB-Instance im Amazon RDS-Benutzerhandbuch.

[RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-mysql-instance-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for MySQL Datenbank-Instance (DB) während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.require_secure_transport` Parameter für die der Instance zugeordnete Parametergruppe auf `0` (aus) gesetzt ist. Dieses Steuerelement bewertet keine RDS-DB-Instances, die Teil eines DB-Clusters sind.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer

Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen dazu, dass alle Verbindungen zu Ihrer RDS for MySQL-DB-Instance SSL verwenden müssen, finden Sie unter SSL/TLS Support für MySQL-DB-Instances auf Amazon RDS im Amazon RDS-Benutzerhandbuch.

[RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-sql-server-logs-to-cloudwatch

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`logTypes`	Eine Liste der Protokolltypen, für deren Veröffentlichung eine RDS for SQL Server-DB-Instance in Logs konfiguriert werden sollte. CloudWatc	EnumList (maximal 2 Elemente)	`agent`, `error`	`agent`, `error`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	h Diese Steuerung schlägt fehl, wenn eine DB-Instance nicht für die Veröffentlichung eines in der Liste angegebenen Protokolltyps konfiguriert ist.			

Dieses Steuerelement prüft, ob eine Amazon RDS for Microsoft SQL Server-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn die RDS for SQL Server-DB-Instance nicht für die Veröffentlichung von Protokollen in CloudWatch Logs konfiguriert ist. Sie können optional die Protokolltypen angeben, für deren Veröffentlichung eine DB-Instance konfiguriert werden soll.

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an eine Amazon RDS-DB-Instance gestellt wurden. Durch die Veröffentlichung von CloudWatch Protokollen in Logs wird die Protokollverwaltung zentralisiert und Sie können Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert Protokolle in einem äußerst langlebigen Speicher. Darüber hinaus können Sie damit Alarme für bestimmte Fehler erstellen, die auftreten können, z. B. bei häufigen Neustarts, die in einem Fehlerprotokoll aufgezeichnet werden. Ebenso können Sie Alarme für Fehler oder Warnungen erstellen, die in SQL Server-Agent-Protokollen aufgezeichnet werden, die sich auf SQL-Agent-Jobs beziehen.

Abhilfe

Informationen zum Veröffentlichen von Protokollen in CloudWatch Logs für eine RDS for SQL Server-DB-Instance finden Sie in den Datenbankprotokolldateien von Amazon RDS for Microsoft SQL Server im Amazon Relational Database Service User Guide.

[RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-sqlserver-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for Microsoft SQL Server-DB-Instance während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.force_ssl` Parameter der Parametergruppe, die der DB-Instance zugeordnet ist, auf gesetzt ist`0 (off)`.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in einem DB-Cluster oder zwischen einem DB-Cluster und einer Client-Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass unbefugte Benutzer den Netzwerkverkehr abhören.

Abhilfe

Informationen SSL/TLS zur Aktivierung von Verbindungen zu Amazon RDS-DB-Instances, auf denen Microsoft SQL Server ausgeführt wird, finden Sie unter Verwenden von SSL mit einer Microsoft SQL Server-DB-Instance im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: mariadb-publish-logs-to-cloudwatch-logs

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`logTypes`	Eine Liste der Protokolltypen, für deren Veröffentlichung eine MariaDB-DB-Instance in Logs konfiguriert werden sollte. CloudWatch Das Steuerelement generiert einen `FAILED` Befund, wenn eine DB-Instance nicht für die Veröffentlichung eines in der Liste angegebenen Protokolltyps konfiguriert ist.	EnumList (maximal 4 Elemente)	`audit`, `error`, `general`, `slowquery`	`audit, error`

Dieses Steuerelement prüft, ob eine Amazon RDS for MariaDB-DB-Instance so konfiguriert ist, dass sie bestimmte Protokolltypen in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn die MariaDB-DB-Instance nicht so konfiguriert ist, dass sie die Protokolle in Logs veröffentlicht. CloudWatch Sie können optional angeben, für welche Arten von Protokollen eine MariaDB-DB-Instance für die Veröffentlichung konfiguriert werden soll.

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an eine Amazon RDS for MariaDB-DB-Instance gestellt wurden. Durch die Veröffentlichung von CloudWatch Protokollen in Amazon Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. Darüber hinaus bewahrt CloudWatch Logs die Protokolle dauerhaft auf, sodass Sicherheits-, Zugriffs- und Verfügbarkeitsprüfungen und Audits unterstützt werden können. Mit CloudWatch Logs können Sie auch Alarme erstellen und Messwerte überprüfen.

Abhilfe

Informationen zur Konfiguration einer Amazon RDS for MariaDB-DB-Instance zur Veröffentlichung von Protokollen in Amazon CloudWatch Logs finden Sie unter Veröffentlichen von MariaDB-

Protokollen in Amazon Logs im Amazon CloudWatch Relational Database Service Service-Benutzerhandbuch.

[RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBProxy`

AWS Config -Regel: rds-proxy-tls-encryption

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Proxy TLS für alle Verbindungen zwischen dem Proxy und der zugrunde liegenden RDS-DB-Instance benötigt. Die Steuerung schlägt fehl, wenn der Proxy nicht TLS für alle Verbindungen zwischen dem Proxy und der RDS-DB-Instance benötigt.

Amazon RDS Proxy kann als zusätzliche Sicherheitsebene zwischen Client-Anwendungen und den zugrunde liegenden RDS-DB-Instances dienen. Sie können beispielsweise mithilfe von TLS 1.3 eine Verbindung zu einem RDS-Proxy herstellen, auch wenn die zugrunde liegende DB-Instance eine ältere Version von TLS unterstützt. Mithilfe von RDS Proxy können Sie strenge Authentifizierungsanforderungen für Datenbankanwendungen durchsetzen.

Abhilfe

Informationen zum Ändern der Einstellungen für einen Amazon RDS-Proxy, sodass TLS erforderlich ist, finden Sie unter Ändern eines RDS-Proxys im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-06.10

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-mariadb-instance-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu einer Amazon RDS for MariaDB-DB-Instance während der Übertragung verschlüsselt werden. Die Steuerung schlägt fehl, wenn die der DB-Instance zugeordnete DB-Parametergruppe nicht synchron ist oder der `require_secure_transport` Parameter der Parametergruppe nicht auf gesetzt ist. `ON`

> **Note**
>
> Dieses Steuerelement bewertet keine Amazon RDS-DB-Instances, die MariaDB-Versionen vor Version 10.5 verwenden. Der `require_secure_transport` Parameter wird nur für MariaDB-Versionen 10.5 und höher unterstützt.

Daten während der Übertragung beziehen sich auf Daten, die von einem Ort zu einem anderen übertragen werden, z. B. zwischen Knoten in einem DB-Cluster oder zwischen einem DB-Cluster und einer Client-Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass unbefugte Benutzer den Netzwerkverkehr abhören.

Abhilfe

Informationen zur Aktivierung SSL/TLS von Verbindungen zu einer Amazon RDS for MariaDB-DB-Instance finden Sie unter Required SSL/TLS for all connections to a MariaDB DB Instance im Amazon Relational Database Service User Guide.

[RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),, NIST.800-53.r5 AU-10, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-12 NIST.800-53.r5 CA-7, (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: aurora-mysql-cluster-audit-logging

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon Aurora MySQL-DB-Cluster die Audit-Protokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die dem DB-Cluster zugeordnete DB-Parametergruppe nicht synchron ist, der `server_audit_logging` Parameter nicht auf 1 gesetzt ist oder der `server_audit_events` Parameter auf einen leeren Wert gesetzt ist.

Datenbankprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen. In Auditprotokollen werden Datenbankaktivitäten aufgezeichnet, darunter Anmeldeversuche, Datenänderungen, Schemaänderungen und andere Ereignisse, die aus Sicherheits- und Compliance-Gründen überprüft werden können.

Abhilfe

Informationen zur Aktivierung der Protokollierung für einen Amazon Aurora MySQL-DB-Cluster finden Sie unter Veröffentlichen von Amazon Aurora CloudWatch MySQL-Protokollen in Amazon Logs im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: rds-instance-subnet-igw-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance in einem öffentlichen Subnetz bereitgestellt wird, das über eine Route zu einem Internet-Gateway verfügt. Die Steuerung schlägt

fehl, wenn die RDS-DB-Instance in einem Subnetz bereitgestellt wird, das über eine Route zu einem Internet-Gateway verfügt und das Ziel auf `0.0.0.0/0` oder gesetzt ist. `::/0`

Durch die Bereitstellung Ihrer Amazon RDS-Ressourcen in privaten Subnetzen können Sie verhindern, dass Ihre RDS-Ressourcen eingehenden Datenverkehr aus dem öffentlichen Internet empfangen, wodurch ein unbeabsichtigter Zugriff auf Ihre RDS-DB-Instances verhindert werden kann. Wenn RDS-Ressourcen in einem öffentlichen Subnetz bereitgestellt werden, das für das Internet zugänglich ist, können sie Risiken wie Datenexfiltration ausgesetzt sein.

Abhilfe

Informationen zur Bereitstellung eines privaten Subnetzes für eine Amazon RDS-DB-Instance finden Sie unter Arbeiten mit einer DB-Instance in einer VPC im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: rds-pgsql-cluster-copy-tags-to-snapshot-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS for PostgreSQL PostgreSQL-DB-Cluster so konfiguriert ist, dass Tags automatisch in Snapshots des DB-Clusters kopiert werden, wenn die Snapshots erstellt werden. Die Steuerung schlägt fehl, wenn der `CopyTagsToSnapshot` Parameter `false` für den RDS for PostgreSQL-DB-Cluster auf gesetzt ist.

Das Kopieren von Tags in DB-Snapshots trägt zur ordnungsgemäßen Ressourcenverfolgung, Steuerung und Kostenzuweisung für alle Backup-Ressourcen bei. Dies ermöglicht eine konsistente Identifizierung von Ressourcen, Zugriffskontrolle und Compliance-Überwachung sowohl für aktive Datenbanken als auch für deren Snapshots. Richtig markierte Snapshots verbessern die Sicherheitsabläufe, indem sie sicherstellen, dass Backup-Ressourcen dieselben Metadaten wie ihre Quelldatenbanken erben.

Abhilfe

Informationen zur Konfiguration eines Amazon RDS for PostgreSQL PostgreSQL-DB-Clusters für das automatische Kopieren von Tags in DB-Snapshots finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: rds-mysql-cluster-copy-tags-to-snapshot-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS for MySQL MySQL-DB-Cluster so konfiguriert ist, dass bei der Erstellung der Snapshots automatisch Tags in Snapshots des DB-Clusters kopiert werden. Die Steuerung schlägt fehl, wenn der `CopyTagsToSnapshot` Parameter `false` für den RDS for MySQL-DB-Cluster auf gesetzt ist.

Das Kopieren von Tags in DB-Snapshots trägt zur ordnungsgemäßen Ressourcenverfolgung, Steuerung und Kostenzuweisung für alle Backup-Ressourcen bei. Dies ermöglicht eine konsistente Identifizierung von Ressourcen, Zugriffskontrolle und Compliance-Überwachung sowohl für aktive Datenbanken als auch für deren Snapshots. Richtig markierte Snapshots verbessern die Sicherheitsabläufe, indem sie sicherstellen, dass Backup-Ressourcen dieselben Metadaten wie ihre Quelldatenbanken erben.

Abhilfe

Informationen zur Konfiguration eines Amazon RDS for MySQL MySQL-DB-Clusters für das automatische Kopieren von Tags in DB-Snapshots finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: rds-cluster-backup-retention-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`minimumBackupRetentionPeriod`	Die Mindestdauer für die Aufbewahrung von Backups in Tagen, die von der Kontrolle überprüft werden muss	Ganzzahl	7 auf 35	7

Dieses Steuerelement prüft, ob ein RDS-DB-Cluster über eine Mindestaufbewahrungsdauer für Backups verfügt. Die Steuerung schlägt fehl, wenn die Aufbewahrungsdauer für Backups unter dem angegebenen Parameterwert liegt. Sofern Sie keinen benutzerdefinierten Parameterwert angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Dieses Steuerelement prüft, ob ein RDS-DB-Cluster über eine Mindestaufbewahrungsdauer für Backups verfügt. Die Steuerung schlägt fehl, wenn die Aufbewahrungsdauer für Backups unter dem angegebenen Parameterwert liegt. Sofern Sie keinen Kundenparameterwert angeben, verwendet Security Hub einen Standardwert von 7 Tagen. Diese Steuerung gilt für alle Arten von RDS-DB-Clustern, einschließlich Aurora-DB-Cluster, DocumentDB-Cluster, NeptuneDB-Cluster usw.

Abhilfe

Um den Aufbewahrungszeitraum für Backups für einen RDS-DB-Cluster zu konfigurieren, ändern Sie die Cluster-Einstellungen und legen Sie den Aufbewahrungszeitraum für Backups auf mindestens 7 Tage (oder den im Steuerparameter angegebenen Wert) fest. Eine ausführliche Anleitung finden Sie unter Aufbewahrungszeitraum für Backup im Amazon Relational Database Service Service-

Benutzerhandbuch. Informationen zu Aurora-DB-Clustern finden Sie unter Überblick über das Sichern und Wiederherstellen eines Aurora-DB-Clusters im Amazon Aurora Aurora-Benutzerhandbuch für Aurora. Für andere Arten von DB-Clustern (z. B. DocumentDB-Cluster) finden Sie im entsprechenden Service-Benutzerhandbuch Informationen zur Aktualisierung der Aufbewahrungsfrist für Backups für den Cluster.

[RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::RDS::GlobalCluster`

AWS Config -Regel: rds-global-cluster-aurora-mysql-supported-version

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0` (nicht anpassbar)
- `longTermSupportVersion`: `8.0.mysql_aurora.3.04.0, 8.0.mysql_aurora.3.04.1, 8.0.mysql_aurora.3.04.2, 8.0.mysql_aurora.3.04.3` (nicht anpassbar)

Diese Kontrolle prüft, ob ein globaler Amazon Aurora MySQL-Cluster auf einer unterstützten Engine-Mindestversion ausgeführt wird. Die Steuerung schlägt fehl, wenn die Version der Aurora MySQL Global Cluster Engine unter der angegebenen unterstützten Mindestversion liegt und nicht im Parameter Version für langfristige Unterstützung aufgeführt ist.

Wenn Sie globale Aurora MySQL-Datenbanken auf unterstützten Engine-Versionen ausführen, können Sie sicherstellen, dass Sie Zugriff auf die neuesten Sicherheitspatches, Bugfixes und Leistungsverbesserungen haben. Für Aurora MySQL-Nebenversionen wurde das Ende des Standard-Supports festgelegt, nach deren Ablauf sie keine wichtigen Patches mehr erhalten. Das Ausführen einer nicht unterstützten Version kann Ihre globale Datenbank Sicherheitslücken aussetzen und zu Gebühren für Amazon RDS Extended Support führen. Da Aurora MySQL einem nicht zusammenhängenden Support-Lebenszyklus folgt, in dem Long-Term Support (LTS) -Versionen länger unterstützt werden als nachfolgende Nicht-LTS-Versionen, sucht diese Steuerung auch nach LTS-Versionen, die noch unter Standardunterstützung fallen. Weitere Informationen finden Sie unter Veröffentlichungskalender für Amazon Aurora MySQL in den Amazon Aurora Aurora-Versionshinweisen für Aurora MySQL.

Abhilfe

Informationen zum Upgrade einer globalen Aurora MySQL-Datenbank auf eine unterstützte Engine-Version finden Sie unter Upgrading an Amazon Aurora Global Database und Upgrading Aurora MySQL by Modification the Engine version im Amazon Aurora Aurora-Benutzerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon Redshift

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Redshift. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-cluster-public-access-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster öffentlich zugänglich sind. Es wertet das `PubliclyAccessible` Feld im Cluster-Konfigurationselement aus.

Das `PubliclyAccessible` Attribut der Amazon Redshift Redshift-Cluster-Konfiguration gibt an, ob der Cluster öffentlich zugänglich ist. Wenn der Cluster mit `PubliclyAccessible` set to konfiguriert ist`true`, handelt es sich um eine Internet-facing Instance mit einem öffentlich auflösbaren DNS-Namen, der in eine öffentliche IP-Adresse aufgelöst wird.

Wenn der Cluster nicht öffentlich zugänglich ist, handelt es sich um eine interne Instanz mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird. Sofern Sie nicht beabsichtigen, dass Ihr Cluster öffentlich zugänglich ist, sollte der Cluster nicht mit der `PubliclyAccessible` Einstellung auf `true` konfiguriert werden.

Abhilfe

Informationen zum Aktualisieren eines Amazon Redshift-Clusters zur Deaktivierung des öffentlichen Zugriffs finden Sie unter Modifizieren eines Clusters im Amazon Redshift Management Guide. Stellen Sie Öffentlich zugänglich auf Nein ein.

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4,, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config -Regel: redshift-require-tls-ssl

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu Amazon Redshift Redshift-Clustern erforderlich sind, um Verschlüsselung bei der Übertragung zu verwenden. Die Prüfung schlägt fehl, wenn der Amazon Redshift Redshift-Clusterparameter `require_SSL` nicht auf `True` gesetzt ist.

TLS kann verwendet werden, um zu verhindern, dass potenzielle Angreifer Person-in-the-Middle- oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über TLS sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Aktualisieren einer Amazon Redshift-Parametergruppe, sodass eine Verschlüsselung erforderlich ist, finden Sie unter Ändern einer Parametergruppe im Amazon Redshift Management Guide. Auf True setzen**`require_ssl`**.

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/PR. DS-11.01

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-backup-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert	
`MinRetentionPeriod`	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	7 auf 35	7	

Dieses Steuerelement prüft, ob in einem Amazon Redshift Redshift-Cluster automatische Snapshots aktiviert sind und ob eine Aufbewahrungsdauer größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn automatische Snapshots für den Cluster nicht aktiviert sind oder wenn die Aufbewahrungsdauer den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub CSPM einen Standardwert von 7 Tagen.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken die Widerstandsfähigkeit Ihrer Systeme. Amazon Redshift erstellt standardmäßig regelmäßig Snapshots. Dieses Steuerelement prüft, ob automatische Snapshots aktiviert sind und mindestens sieben Tage lang aufbewahrt werden. Weitere Informationen zu automatisierten Amazon Redshift-Snapshots finden Sie unter Automatisierte Snapshots im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Aktualisierung der Aufbewahrungsdauer von Snapshots für einen Amazon Redshift-Cluster finden Sie unter Modifizieren eines Clusters im Amazon Redshift Management Guide. Stellen Sie für Backup die Snapshot-Aufbewahrung auf einen Wert von 7 oder höher ein.

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config Regel: `redshift-cluster-audit-logging-enabled` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon Redshift Redshift-Cluster die Audit-Protokollierung aktiviert ist.

Die Amazon Redshift Redshift-Audit-Protokollierung bietet zusätzliche Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Cluster. Diese Daten können in Amazon S3 gespeichert und gesichert werden und können bei Sicherheitsüberprüfungen und Untersuchungen hilfreich sein. Weitere Informationen finden Sie unter Protokollierung von Datenbankprüfungen im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Konfiguration der Audit-Protokollierung für einen Amazon Redshift-Cluster finden Sie unter Konfiguration der Überwachung mithilfe der Konsole im Amazon Redshift Management Guide.

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), CRI-Profil v2. 2/PR. PS-02.01, CRI-Profil v2. 2/PR. PS-02.03

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-cluster-maintenancesettings-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `allowVersionUpgrade = true`(nicht anpassbar)

Dieses Steuerelement prüft, ob automatische Hauptversions-Upgrades für den Amazon Redshift Redshift-Cluster aktiviert sind.

Durch die Aktivierung automatischer Hauptversions-Upgrades wird sichergestellt, dass die neuesten Hauptversionsupdates für Amazon Redshift Redshift-Cluster während des Wartungsfensters installiert werden. Diese Updates können Sicherheitspatches und Fehlerkorrekturen beinhalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Abhilfe

Um dieses Problem von zu beheben AWS CLI, verwenden Sie den Amazon Redshift `modify-cluster` Redshift-Befehl und legen Sie das `--allow-version-upgrade` Attribut fest. *`clustername`*ist der Name Ihres Amazon Redshift Redshift-Clusters.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI Profile v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-enhanced-vpc-routing-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster `EnhancedVpcRouting` aktiviert wurde.

Durch das verbesserte VPC-Routing wird der gesamte `COPY` `UNLOAD` Datenverkehr zwischen dem Cluster und den Datenrepositorys über Ihre VPC geleitet. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können VPC Flow Logs auch verwenden, um den Netzwerkverkehr zu überwachen.

Abhilfe

Detaillierte Anweisungen zur Problembehebung finden Sie unter Enabling enhanced VPC Routing im Amazon Redshift Management Guide.

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. AA-01.01

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-default-admin-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Diese Steuerung schlägt fehl, wenn der Admin-Benutzername für einen Redshift-Cluster auf `awsuser` gesetzt ist.

Wenn Sie einen Redshift-Cluster erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Sie können den Admin-Benutzernamen für Ihren Amazon Redshift Redshift-Cluster nicht ändern, nachdem Sie ihn erstellt haben. Informationen zum Erstellen eines neuen Clusters mit einem nicht standardmäßigen Benutzernamen finden Sie unter Schritt 1: Erstellen eines Amazon Redshift-Beispielclusters im Amazon Redshift Getting Started Guide.

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-cluster-kms-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster im Ruhezustand verschlüsselt sind. Die Steuerung schlägt fehl, wenn ein Redshift-Cluster im Ruhezustand nicht verschlüsselt ist

oder wenn sich der Verschlüsselungsschlüssel von dem im Regelparameter angegebenen Schlüssel unterscheidet.

In Amazon Redshift können Sie die Datenbankverschlüsselung für Ihre Cluster aktivieren, um Data-at-Rest besser zu schützen. Wenn Sie die Verschlüsselung für einen Cluster aktivieren, werden die Datenblöcke und die Metadaten des Systems für den Cluster und Snapshots des Clusters verschlüsselt. Die Verschlüsselung von Daten im Ruhezustand ist eine empfohlene bewährte Methode, da sie Ihren Daten eine Ebene der Zugriffsverwaltung hinzufügt. Die Verschlüsselung ruhender Redshift-Cluster reduziert das Risiko, dass ein nicht autorisierter Benutzer auf die auf der Festplatte gespeicherten Daten zugreifen kann.

Abhilfe

Informationen zur Änderung eines Redshift-Clusters für die Verwendung der KMS-Verschlüsselung finden Sie unter Ändern der Cluster-Verschlüsselung im Amazon Redshift Management Guide.

[Redshift.11] Redshift-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config Regel: `tagged-redshift-cluster` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::EventSubscription`

AWS Config Regel: `tagged-redshift-eventsubscription` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Abonnement für Redshift-Ereignisbenachrichtigungen finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSnapshot`

AWS Config Regel: `tagged-redshift-clustersnapshot` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	`No default value`

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster-Snapshot finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSubnetGroup`

AWS Config Regel: `tagged-redshift-clustersubnetgroup` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine Amazon Redshift Redshift-Cluster-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Cluster-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Cluster-Subnetzgruppe mit keinem Schlüssel

gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Redshift-Cluster-Subnetzgruppe finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

Verwandte Anforderungen: PCI DSS v4.0. 1/13.3.1, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-unrestricted-port-access

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine mit einem Amazon Redshift Redshift-Cluster verknüpfte Sicherheitsgruppe über Eingangsregeln verfügt, die den Zugriff auf den Cluster-Port über das Internet zulassen (0.0.0). 0/0 oder: :/0). Die Steuerung schlägt fehl, wenn die Zugriffsregeln der Sicherheitsgruppe den Zugriff auf den Cluster-Port über das Internet zulassen.

Die Zulassung eines uneingeschränkten eingehenden Zugriffs auf den Redshift-Cluster-Port (IP-Adresse mit dem Suffix /0) kann zu unbefugtem Zugriff oder Sicherheitsvorfällen führen. Wir empfehlen, bei der Erstellung von Sicherheitsgruppen und der Konfiguration von Regeln für eingehenden Datenverkehr das Prinzip des Zugriffs mit den geringsten Rechten anzuwenden.

Abhilfe

Informationen zur Beschränkung des Eingangs auf dem Redshift-Cluster-Port auf eingeschränkte Ursprünge finden Sie unter Arbeiten mit Sicherheitsgruppenregeln im Amazon VPC-Benutzerhandbuch. Aktualisieren Sie Regeln, bei denen der Portbereich mit dem Redshift-Cluster-Port übereinstimmt und der IP-Portbereich 0,0.0 ist. 0/0.

[Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben

Verwandte Anforderungen: CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::ClusterSubnetGroup`

AWS Config -Regel: redshift-cluster-subnet-group-multi-az

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Die Steuerung prüft, ob eine Amazon Redshift Redshift-Cluster-Subnetzgruppe Subnetze aus mehr als einer Availability Zone (AZ) hat. Die Steuerung schlägt fehl, wenn die Cluster-Subnetzgruppe keine Subnetze von mindestens zwei verschiedenen AZs hat.

Durch die Konfiguration von Subnetzen über mehrere AZs hinweg wird sichergestellt, dass Ihr Redshift Data Warehouse auch bei Ausfällen weiterbetrieben werden kann.

Abhilfe

Informationen zum Ändern einer Redshift-Cluster-Subnetzgruppe, sodass sie sich über mehrere AZs erstreckt, finden Sie unter Ändern einer Cluster-Subnetzgruppe im Amazon Redshift Management Guide.

[Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterParameterGroup`

AWS Config -Regel: redshift-cluster-parameter-group-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	Groß- und Kleinschreibung unterschieden.			

Dieses Steuerelement prüft, ob eine Amazon Redshift Redshift-Cluster-Parametergruppe die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel hat. Die Steuerung schlägt fehl, wenn die Parametergruppe keine Tag-Schlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Parametergruppe keine Tag-Schlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon Redshift-Cluster-Parametergruppe finden Sie unter Tag-Ressourcen in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/GV. OC-04.03, CRI-Profil v2. 2/GV. RM-09.02, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: redshift-cluster-multi-az-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob mehrere Availability Zones (Multi-AZ) -Bereitstellungen für einen Amazon Redshift Redshift-Cluster aktiviert sind. Die Steuerung schlägt fehl, wenn Multi-AZ Bereitstellungen für den Amazon Redshift Redshift-Cluster nicht aktiviert sind.

Amazon Redshift unterstützt mehrere Availability Zones (Multi-AZ) -Bereitstellungen für bereitgestellte Cluster. Wenn Multi-AZ Bereitstellungen für einen Cluster aktiviert sind, kann ein Amazon Redshift Data Warehouse in Ausfallszenarien weiterarbeiten, wenn in einer Availability Zone (AZ) ein unerwartetes Ereignis eintritt. Eine Multi-AZ Bereitstellung stellt Rechenressourcen in mehr als einer AZ bereit, und auf diese Rechenressourcen kann über einen einzigen Endpunkt zugegriffen werden. Im Falle eines vollständigen AZ-Ausfalls sind die verbleibenden Rechenressourcen in einer anderen AZ verfügbar, um die Verarbeitung von Workloads fortzusetzen. Sie können ein vorhandenes Single-AZ Data Warehouse in ein Multi-AZ Data Warehouse konvertieren. Zusätzliche Rechenressourcen werden dann in einer zweiten AZ bereitgestellt.

Abhilfe

Informationen zur Konfiguration von Multi-AZ Bereitstellungen für einen Amazon Redshift-Cluster finden Sie unter Konvertieren eines Single-AZ Data Warehouse in ein Multi-AZ Data Warehouse im Amazon Redshift Management Guide.

Security Hub CSPM-Steuerelemente für Amazon Redshift Serverless

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Redshift Serverless. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

Verwandte Anforderungen: CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-06.10

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::RedshiftServerless::Workgroup`

AWS Config -Regel: redshift-serverless-workgroup-routes-within-vpc

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob erweitertes VPC-Routing für eine Amazon Redshift Serverless-Arbeitsgruppe aktiviert ist. Die Steuerung schlägt fehl, wenn das erweiterte VPC-Routing für die Arbeitsgruppe deaktiviert ist.

Wenn erweitertes VPC-Routing für eine Amazon Redshift Serverless-Arbeitsgruppe deaktiviert ist, leitet Amazon Redshift den Datenverkehr über das Internet weiter, einschließlich des Datenverkehrs zu anderen Diensten innerhalb des Netzwerks. AWS Wenn Sie erweitertes VPC-Routing für eine Arbeitsgruppe aktivieren, zwingt Amazon Redshift den gesamten `UNLOAD` Datenverkehr zwischen Ihrem Cluster `COPY` und Ihren Datenrepositorys über Ihre Virtual Private Cloud (VPC), die auf dem Amazon VPC-Service basiert. Mit erweitertem VPC-Routing können Sie Standard-VPC-Funktionen verwenden, um den Datenfluss zwischen Ihrem Amazon Redshift Redshift-Cluster und anderen Ressourcen zu steuern. Dazu gehören Funktionen wie VPC-Sicherheitsgruppen und Endpunktrichtlinien, Network Access Control Lists (ACLs) und Domain Name System (DNS) -Server. Sie können auch VPC-Flow-Logs verwenden, um den `UNLOAD` Datenverkehr `COPY` zu überwachen.

Abhilfe

Weitere Informationen über erweitertes VPC-Routing und dessen Aktivierung für eine Arbeitsgruppe finden Sie unter Steuern des Netzwerkverkehrs mit erweitertem Redshift-VPC-Routing im Amazon Redshift Management Guide.

[RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein

Verwandte Anforderungen: CRI Profile v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::RedshiftServerless::Workgroup`

AWS Config -Regel: redshift-serverless-workgroup-encrypted-in-transit

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu einer Amazon Redshift Serverless-Arbeitsgruppe erforderlich sind, um Daten während der Übertragung zu verschlüsseln. Die Steuerung schlägt fehl, wenn der `require_ssl` Konfigurationsparameter für die Arbeitsgruppe auf gesetzt ist. `false`

Eine Amazon Redshift Serverless-Arbeitsgruppe ist eine Sammlung von Rechenressourcen, die Rechenressourcen wie RPUs, VPC-Subnetzgruppen und Sicherheitsgruppen gruppiert. Zu den Eigenschaften einer Arbeitsgruppe gehören Netzwerk- und Sicherheitseinstellungen. Diese Einstellungen geben an, ob Verbindungen zu einer Arbeitsgruppe erforderlich sein sollen, um SSL zur Verschlüsselung von Daten während der Übertragung zu verwenden.

Abhilfe

Informationen zur Aktualisierung der Einstellungen für eine Amazon Redshift Serverless-Arbeitsgruppe, sodass SSL-Verbindungen erforderlich sind, finden Sie unter Connecting to Amazon Redshift Serverless im Amazon Redshift Management Guide.

[RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: CRI Profile v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. DS-01.02, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::RedshiftServerless::Workgroup`

AWS Config -Regel: redshift-serverless-workgroup-no-public-access

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der öffentliche Zugriff für eine Amazon Redshift Serverless-Arbeitsgruppe deaktiviert ist. Es bewertet die `publiclyAccessible` Eigenschaft einer Redshift Serverless-Arbeitsgruppe. Die Steuerung schlägt fehl, wenn der öffentliche Zugriff für die Arbeitsgruppe aktiviert ist (`true`).

Die Einstellung public access (`publiclyAccessible`) für eine Amazon Redshift Serverless-Arbeitsgruppe gibt an, ob auf die Arbeitsgruppe von einem öffentlichen Netzwerk aus zugegriffen werden kann. Wenn der öffentliche Zugriff für eine Arbeitsgruppe aktiviert (`true`) ist, erstellt Amazon Redshift eine Elastic IP-Adresse, die die Arbeitsgruppe von außerhalb der VPC öffentlich zugänglich macht. Wenn Sie nicht möchten, dass eine Arbeitsgruppe öffentlich zugänglich ist, deaktivieren Sie den öffentlichen Zugriff für sie.

Abhilfe

Informationen zum Ändern der öffentlichen Zugriffseinstellungen für eine Amazon Redshift Serverless-Arbeitsgruppe finden Sie unter Anzeigen der Eigenschaften für eine Arbeitsgruppe im Amazon Redshift Management Guide.

[RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), (2),, NIST.800-53.r5 SC-12 (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (6) NIST.800-53.r5 SI-7

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::RedshiftServerless::Namespace`

AWS Config -Regel: redshift-serverless-namespace-cmk-encryption

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`kmsKeyArns`	Eine Liste der Amazon-Ressourcennamen (ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerelement generiert einen `FAILED` Befund, wenn ein Redshift Serverless-Namespace nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.	StringList (maximal 3 Elemente)	1—3 ARNs vorhandener KMS-Schlüssel. Beispiel: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Redshift Serverless-Namespace im Ruhezustand verschlüsselt ist, wenn ein Kunde verwaltet wird. AWS KMS key Die Steuerung schlägt fehl, wenn der Redshift Serverless-Namespace nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

In Amazon Redshift Serverless definiert ein Namespace einen logischen Container für Datenbankobjekte. Dieses Steuerelement überprüft regelmäßig, ob die Verschlüsselungseinstellungen für einen Namespace einen vom Kunden verwalteten AWS KMS key anstelle eines AWS verwalteten KMS-Schlüssels für die Verschlüsselung von Daten im Namespace angeben. Mit einem vom Kunden verwalteten KMS-Schlüssel haben Sie die volle Kontrolle über den Schlüssel. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von

Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels.

Abhilfe

Informationen zur Aktualisierung der Verschlüsselungseinstellungen für einen Amazon Redshift Serverless Namespace und zur Angabe eines vom Kunden verwalteten AWS KMS key Namespace finden Sie unter Ändern des AWS KMS key für einen Namespace im Amazon Redshift Management Guide.

[RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RedshiftServerless::Namespace`

AWS Config -Regel: redshift-serverless-default-admin-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Admin-Benutzername für einen Amazon Redshift Serverless-Namespace der Standard-Admin-Benutzername ist. `admin` Die Steuerung schlägt fehl, wenn der Admin-Benutzername für den Redshift Serverless-Namespace lautet. `admin`

Wenn Sie einen Amazon Redshift Serverless-Namespace erstellen, sollten Sie einen benutzerdefinierten Admin-Benutzernamen für den Namespace angeben. Der standardmäßige Admin-Benutzername ist public knowledge. Durch die Angabe eines benutzerdefinierten Admin-Benutzernamens können Sie beispielsweise dazu beitragen, das Risiko oder die Effektivität von Brute-Force-Angriffen gegen den Namespace zu verringern.

Abhilfe

Sie können den Admin-Benutzernamen für einen Amazon Redshift Serverless-Namespace mithilfe der Amazon Redshift Serverless-Konsole oder API ändern. Um ihn mithilfe der Konsole zu ändern, wählen Sie die Namespace-Konfiguration und dann im Menü Aktionen die Option Administratoranmeldedaten bearbeiten aus. Um ihn programmgesteuert zu ändern, verwenden Sie den UpdateNamespaceVorgang oder, falls Sie den verwenden AWS CLI, führen Sie den Befehl

update-namespace aus. Wenn Sie den Admin-Benutzernamen ändern, müssen Sie gleichzeitig auch das Admin-Passwort ändern.

[RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RedshiftServerless::Namespace`

AWS Config -Regel: redshift-serverless-publish-logs-to-cloudwatch

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Serverless Namespace so konfiguriert ist, dass er Verbindungs- und Benutzerprotokolle nach Amazon Logs exportiert. CloudWatch Die Steuerung schlägt fehl, wenn der Redshift Serverless-Namespace nicht für den Export der Protokolle in Logs konfiguriert ist. CloudWatch

Wenn Sie Amazon Redshift Serverless so konfigurieren, dass Verbindungsprotokoll- (`connectionlog`) und Benutzerprotokolldaten (`userlog`) in eine Protokollgruppe in Amazon CloudWatch Logs exportiert werden, können Sie Ihre Protokolldatensätze sammeln und in einem dauerhaften Speicher speichern, der Sicherheits-, Zugriffs- und Verfügbarkeitsprüfungen und Audits unterstützt. Mit CloudWatch Logs können Sie auch Protokolldaten in Echtzeit analysieren und diese zur Erstellung von Alarmen und CloudWatch zur Überprüfung von Metriken verwenden.

Abhilfe

Um Protokolldaten für einen Amazon Redshift Serverless-Namespace nach Amazon CloudWatch Logs zu exportieren, müssen die entsprechenden Protokolle in den Konfigurationseinstellungen für die Auditprotokollierung für den Namespace für den Export ausgewählt werden. Informationen zur Aktualisierung dieser Einstellungen finden Sie unter Sicherheit und Verschlüsselung bearbeiten im Amazon Redshift Management Guide.

Security Hub CSPM-Steuerelemente für Route 53

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Route 53.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Route53.1] Route 53-Gesundheitschecks sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Route53::HealthCheck`

AWS Config Regel: `tagged-route53-healthcheck` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Route 53-Zustandsprüfung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Zustandsprüfung keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter

angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Zustandsprüfung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Route 53-Zustandsprüfung finden Sie unter Benennen und Markieren von Zustandsprüfungen im Amazon Route 53-Entwicklerhandbuch.

[Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Route53::HostedZone`

AWS Config -Regel: `route53-query-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die DNS-Abfrageprotokollierung für eine öffentlich gehostete Zone von Amazon Route 53 aktiviert ist. Die Steuerung schlägt fehl, wenn die DNS-Abfrageprotokollierung für eine öffentlich gehostete Route 53-Zone nicht aktiviert ist.

Das Protokollieren von DNS-Abfragen für eine von Route 53 gehostete Zone entspricht den DNS-Sicherheits- und Compliance-Anforderungen und sorgt für Transparenz. Die Protokolle enthalten Informationen wie die abgefragte Domäne oder Subdomäne, Datum und Uhrzeit der Abfrage, den DNS-Eintragstyp (z. B. A oder AAAA) und den DNS-Antwortcode (z. B. oder). `NoError` `ServFail` Wenn die DNS-Abfrageprotokollierung aktiviert ist, veröffentlicht Route 53 die Protokolldateien in Amazon CloudWatch Logs.

Abhilfe

Informationen zum Protokollieren von DNS-Abfragen für öffentlich gehostete Route 53-Zonen finden Sie unter Konfiguration der Protokollierung für DNS-Abfragen im Amazon Route 53-Entwicklerhandbuch.

Security Hub CSPM-Steuerelemente für Amazon S3

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Storage Service (Amazon S3). Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/21.1.4, Benchmark v3.0 für CIS AWS Foundations. 0/21.1.4, Benchmark für CIS AWS Foundations v1.4. 0/2.1.5, NIST.800-53.r5

AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: s3-account-level-public-access-blocks-periodic

Art des Zeitplans: Periodisch

Parameter:

- `ignorePublicAcls`: `true` (nicht anpassbar)
- `blockPublicPolicy`: `true` (nicht anpassbar)
- `blockPublicAcls`: `true` (nicht anpassbar)
- `restrictPublicBuckets`: `true` (nicht anpassbar)

Diese Kontrolle prüft, ob die oben genannten Amazon S3 S3-Einstellungen für den öffentlichen Zugriff blockieren auf Kontoebene für einen S3-Allzweck-Bucket konfiguriert sind. Die Steuerung schlägt fehl, wenn eine oder mehrere der Einstellungen zum Blockieren des öffentlichen Zugriffs auf gesetzt sind`false`.

Die Steuerung schlägt fehl`false`, wenn eine der Einstellungen auf eingestellt ist oder wenn eine der Einstellungen nicht konfiguriert ist.

Amazon S3 Public Access Block wurde entwickelt, um Kontrollen auf der gesamten AWS-Konto oder auf der Ebene einzelner S3-Buckets bereitzustellen, um sicherzustellen, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Kontoebene konfigurieren.

Weitere Informationen finden Sie unter Verwenden von Amazon S3 Block Public Access im Amazon Simple Storage Service-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von Amazon S3 Block Public Access für Sie AWS-Konto finden Sie unter Konfiguration der Einstellungen für den Block Public Access für Ihr Konto im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-public-read-prohibited

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Lesezugriff gewährt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Lesezugriff gewährt.

> **Note**
>
> Wenn ein S3-Bucket über eine Bucket-Richtlinie verfügt, wertet dieses Steuerelement keine Richtlinienbedingungen aus, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Bucket-Richtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten.

Informationen zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

In einigen Anwendungsfällen kann es erforderlich sein, dass jeder im Internet aus Ihrem S3-Bucket lesen kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich lesbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Lesezugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

Verwandte Anforderungen: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-public-write-prohibited

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Schreibzugriff zulässt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Schreibzugriff zulässt.

> **Note**
>
> Wenn ein S3-Bucket über eine Bucket-Richtlinie verfügt, wertet dieses Steuerelement keine Richtlinienbedingungen aus, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Bucket-Richtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

Einige Anwendungsfälle erfordern, dass jeder im Internet in den S3-Bucket schreiben kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich beschreibbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Schreibzugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/21.1.1, Benchmark v3.0 für CIS AWS Foundations. 0/21.1.1, Benchmark für CIS AWS Foundations v1.4. 0/2.1.2, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4),, NIST.800-53.r5 SC-7 (1), (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, 3.13.15, PCI DSS NIST.800-171.r2 v3.2. 1/41.1, PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-ssl-requests-only

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Richtlinie verfügt, nach der Anfragen TLS verwenden müssen. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie keine Anfragen zur Verwendung von TLS erfordert.

S3-Buckets sollten über Richtlinien verfügen, die vorschreiben, dass alle Anfragen (`Action: S3:*`) in der S3-Ressourcenrichtlinie, wie durch den Bedingungsschlüssel `aws:SecureTransport` angegeben, nur die Übertragung von Daten über HTTPS akzeptieren.

Abhilfe

Informationen zur Aktualisierung einer Amazon S3 S3-Bucket-Richtlinie, um unsicheren Transport zu verweigern, finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

Fügen Sie eine Richtlinienerklärung hinzu, die der in der folgenden Richtlinie ähnelt. `amzn-s3-demo-bucket`Ersetzen Sie es durch den Namen des Buckets, den Sie ändern.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
```

```
}
```

Weitere Informationen finden Sie unter Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config Regel s3-bucket-ssl-requests-only einzuhalten? im offiziellen Knowledge Center.AWS

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.13.4 NIST.800-53.r5 CM-2, CRI-Profil v2. 2/PR. AA-05.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Eingeschränkte Aktionen für sensible API-Operationen

Schweregrad: Hoch

Art der Ressource: `AWS::S3::Bucket`

AWS Config-Regel: s3-bucket-blacklisted-actions-prohibited

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (nicht anpassbar)

Diese Kontrolle prüft, ob eine allgemeine Amazon S3 S3-Bucket-Richtlinie verhindert, dass Prinzipale AWS-Konten anderer Benutzer verweigerte Aktionen für Ressourcen im S3-Bucket ausführen. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie eine oder mehrere der vorherigen Aktionen für einen Prinzipal in einem anderen AWS-Konto zulässt.

Die Implementierung des Zugriffs mit den geringsten Rechten ist von grundlegender Bedeutung, um das Sicherheitsrisiko und die Auswirkungen von Fehlern oder böswilligen Absichten zu verringern. Wenn eine S3-Bucket-Richtlinie den Zugriff von externen Konten aus ermöglicht, kann dies zu einer Datenexfiltration durch eine Insider-Bedrohung oder einen Angreifer führen.

Der `blacklistedactionpatterns` Parameter ermöglicht eine erfolgreiche Auswertung der Regel für S3-Buckets. Der Parameter gewährt Zugriff auf externe Konten für Aktionsmuster, die nicht in der `blacklistedactionpatterns` Liste enthalten sind.

Abhilfe

Informationen zum Aktualisieren einer Amazon S3 S3-Bucket-Richtlinie zum Entfernen von Berechtigungen finden Sie unter. Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie auf der Seite Bucket-Richtlinie bearbeiten im Textfeld zur Richtlinienbearbeitung eine der folgenden Aktionen aus:

- Entfernen Sie die Anweisungen, die anderen AWS-Konten Zugriff auf verweigerte Aktionen gewähren.
- Entfernen Sie die zulässigen verweigerten Aktionen aus den Anweisungen.

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

Verwandte Anforderungen: PCI DSS v3.2. 1/2.2, NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (1) NIST.800-53.r5 CP-6, (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-36 (2), NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/GV. OC-05.03, CRI-Profil v2. 2/GV. OC-05.04, CRI-Profil v2. 2/PR. DS-11.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02, CRI-Profil v2. 2/RC. RP-03.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: s3-bucket-cross-region-replication-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die regionsübergreifende Replikation aktiviert ist. Die Steuerung schlägt fehl, wenn für den Bucket keine regionsübergreifende Replikation aktiviert ist.

Bei der Replikation handelt es sich um das automatische, asynchrone Kopieren von Objekten zwischen Buckets desselben oder eines anderen. AWS-Regionen Bei der Replikation werden neu erstellte Objekte und Objektaktualisierungen von einem Quell-Bucket in einen oder mehrere Ziel-

Buckets kopiert. AWS In bewährten Verfahren wird die Replikation für Quell- und Ziel-Buckets empfohlen, die demselben Eigentümer gehören. AWS-Konto Zusätzlich zur Verfügbarkeit sollten Sie andere Einstellungen für die Systemstabilisierung berücksichtigen.

Dieses Steuerelement generiert einen `FAILED` Befund für einen Replizierungsziel-Bucket, wenn für diesen keine regionsübergreifende Replikation aktiviert ist. Wenn es einen legitimen Grund dafür gibt, dass für die Aktivierung des Ziel-Buckets keine regionsübergreifende Replikation erforderlich ist, können Sie die Ergebnisse für diesen Bucket unterdrücken.

Abhilfe

Informationen zum Aktivieren der Cross-Region Replikation auf einem S3-Bucket finden Sie unter Konfiguration der Replikation für Quell- und Ziel-Buckets, die demselben Konto gehören, im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie für Quell-Bucket die Option Auf alle Objekte im Bucket anwenden aus.

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/21.1.4, Benchmark CIS AWS GUS-Stiftungen v3.0.02.1.4, Benchmark CIS GUS-Stiftungen v1.4. AWS 0/2.1.5,, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0 NIST.800-53.r5 SC-7. 1/1.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.03, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Hoch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-level-public-access-prohibited

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludedPublicBuckets`(nicht anpassbar) — Eine durch Kommas getrennte Liste bekannter zulässiger öffentlicher S3-Bucket-Namen

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket den öffentlichen Zugriff auf Bucket-Ebene blockiert. Die Steuerung schlägt fehl, wenn eine der folgenden Einstellungen auf gesetzt istfalse:

- ignorePublicAcls
- blockPublicPolicy
- blockPublicAcls
- restrictPublicBuckets

Block Public Access auf S3-Bucket-Ebene bietet Kontrollen, mit denen sichergestellt wird, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Bucket-Ebene konfigurieren.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf Bucket-Ebene finden Sie unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher im Amazon S3 S3-Benutzerhandbuch.

[S3.9] Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 NIST.800-171.r2 3.3.8, PCI DSS v4.0. 1/102.2.1, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: s3-bucket-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für einen Amazon S3 S3-Allzweck-Bucket aktiviert ist. Die Steuerung schlägt fehl, wenn die Serverzugriffsprotokollierung nicht aktiviert ist. Wenn die Protokollierung aktiviert ist, übermittelt Amazon S3 Zugriffsprotokolle für einen Quell-Bucket an einen ausgewählten Ziel-Bucket. Der Ziel-Bucket muss sich im selben AWS-Region wie der Quell-Bucket befinden und es darf kein standardmäßiger Aufbewahrungszeitraum konfiguriert sein. Für den Ziel-Logging-Bucket muss die Serverzugriffsprotokollierung nicht aktiviert sein, und Sie sollten die Ergebnisse für diesen Bucket unterdrücken.

Die Serverzugriffsprotokollierung bietet detaillierte Aufzeichnungen der Anfragen, die an einen Bucket gestellt wurden. Serverzugriffsprotokolle können bei Sicherheits- und Zugriffsprüfungen hilfreich sein. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon S3: Aktivieren Sie die Amazon S3 S3-Serverzugriffsprotokollierung.

Abhilfe

Informationen zur Aktivierung der Amazon S3 S3-Serverzugriffsprotokollierung finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung im Amazon S3 S3-Benutzerhandbuch.

[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/ID. AM-08.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-version-lifecycle-policy-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein versionsbasierter Amazon S3 S3-Bucket für allgemeine Zwecke über eine Lifecycle-Konfiguration verfügt. Die Kontrolle schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat.

Wir empfehlen, eine Lifecycle-Konfiguration für Ihren S3-Bucket zu erstellen, um Ihnen bei der Definition von Aktionen zu helfen, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll.

> **Tip**
>
> Die Aktivierung der Versionierung ohne Lebenszyklusmanagement kann zu unbegrenztem Speicherwachstum und höheren Kosten führen. Bei jeder Objektänderung wird eine neue Version erstellt, die auf unbestimmte Zeit beibehalten wird. Konfigurieren Sie S3-Lebenszyklusregeln so, dass ältere Versionen automatisch auf günstigere Speicherklassen umgestellt werden oder sie nach einem definierten Aufbewahrungszeitraum ablaufen.

Abhilfe

Weitere Informationen zur Konfiguration des Lebenszyklus in einem Amazon S3 S3-Bucket finden Sie unter Verwenden der S3-Versionierung mit dem S3-Lebenszyklus, Einrichten der Lebenszykluskonfiguration für einen Bucket und Verwalten des Lebenszyklus von Objekten im Amazon S3 S3-Benutzerhandbuch.

[S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4), NIST.800-171.r2 3.3.8, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-event-notifications-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`eventTypes`	Liste der bevorzugten S3-Ereignistypen	EnumList (maximal 28 Artikel)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`, `s3:ObjectAcl:Put`, `s3:ObjectCreated:*`, `s3:ObjectCreated:CompleteMultipartUpload`, `s3:ObjectCreated:Copy`,	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
			s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*,	

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
			s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold,	

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
			`s3:TestEvent`	

Dieses Steuerelement prüft, ob S3-Ereignisbenachrichtigungen in einem Amazon S3 S3-Allzweck-Bucket aktiviert sind. Die Steuerung schlägt fehl, wenn S3-Ereignisbenachrichtigungen für den Bucket nicht aktiviert sind. Wenn Sie benutzerdefinierte Werte für den `eventTypes` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn Ereignisbenachrichtigungen für die angegebenen Ereignistypen aktiviert sind.

Wenn Sie S3-Ereignisbenachrichtigungen aktivieren, erhalten Sie Benachrichtigungen, wenn bestimmte Ereignisse eintreten, die sich auf Ihre S3-Buckets auswirken. Sie können beispielsweise über die Erstellung, Entfernung von Objekten und Wiederherstellung von Objekten informiert werden. Diese Benachrichtigungen können die zuständigen Teams vor versehentlichen oder vorsätzlichen Änderungen warnen, die zu unberechtigtem Datenzugriff führen können.

Abhilfe

Informationen zum Erkennen von Änderungen an S3-Buckets und Objekten finden Sie unter Amazon S3 S3-Ereignisbenachrichtigungen im Amazon S3 S3-Benutzerhandbuch.

[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-acl-prohibited

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket Benutzerberechtigungen mit einer Zugriffskontrollliste (ACL) bereitstellt. Die Kontrolle schlägt fehl, wenn eine ACL für die Verwaltung des Benutzerzugriffs auf den Bucket konfiguriert ist.

ACLs sind veraltete Zugriffskontrollmechanismen, die älter als IAM sind. Anstelle von ACLs empfehlen wir, S3-Bucket-Richtlinien oder AWS Identity and Access Management (IAM-) Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets zu verwalten.

Abhilfe

Um diese Kontrolle zu umgehen, sollten Sie ACLs für Ihre S3-Buckets deaktivieren. Anweisungen finden Sie unter Kontrolle des Besitzes von Objekten und Deaktivieren von ACLs für Ihren Bucket im Amazon Simple Storage Service-Benutzerhandbuch.

Informationen zum Erstellen einer S3-Bucket-Richtlinie finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole. Informationen zum Erstellen einer IAM-Benutzerrichtlinie für einen S3-Bucket finden Sie unter Steuern des Zugriffs auf einen Bucket mit Benutzerrichtlinien.

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), CRI-Profil v2. 2/ID. AM-08.01

Kategorie: Schützen > Datenschutz

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-lifecycle-policy-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`targetTransitionDays`	Anzahl der Tage nach der Objekterstellung, an denen Objekte in eine bestimmte Speicherklasse umgestellt wurden	Ganzzahl	1 auf 36500	Kein Standardwert
`targetExpirationDays`	Anzahl der Tage nach der Objekterstellung, an denen Objekte gelöscht werden	Ganzzahl	1 auf 36500	Kein Standardwert
`targetTransitionStorageClass`	Typ der S3-Speicherklasse des Ziels	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Lifecycle-Konfiguration verfügt. Die Steuerung schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat. Wenn Sie benutzerdefinierte Werte für einen oder mehrere der oben genannten Parameter angeben, ist die Kontrolle nur erfolgreich, wenn die Richtlinie die angegebene Speicherklasse, Löschzeit oder Übergangszeit beinhaltet.

Durch das Erstellen einer Lifecycle-Konfiguration für Ihren S3-Bucket werden Aktionen definiert, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll. Sie können beispielsweise

Objekte in eine andere Speicherklasse übertragen, archivieren oder nach einem bestimmten Zeitraum löschen.

Abhilfe

Informationen zur Konfiguration von Lebenszyklusrichtlinien für einen Amazon S3 S3-Bucket finden Sie unter Einstellung der Lebenszykluskonfiguration für einen Bucket und unter Verwaltung Ihres Speicherlebenszyklus im Amazon S3 S3-Benutzerhandbuch.

[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.r5 AU-9 (2),, NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.3.8, CRI Profile v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. PS-01.03

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-versioning-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die Versionierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Versionierung für den Bucket ausgesetzt ist.

Bei der Versionierung werden mehrere Varianten eines Objekts im selben S3-Bucket aufbewahrt. Sie können die Versionierung verwenden, um alle Versionen aller in Ihrem S3-Bucket gespeicherten Objekte beizubehalten, abzurufen und wiederherzustellen. Die Versionierung hilft Ihnen bei der Wiederherstellung sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern.

> **Tip**
>
> Die Aktivierung der Versionierung ohne Lebenszyklusmanagement kann zu unbegrenztem Speicherwachstum und höheren Kosten führen. Bei jeder Objektänderung wird eine neue Version erstellt, die auf unbestimmte Zeit beibehalten wird. Konfigurieren Sie S3-

Lebenszyklusregeln so, dass ältere Versionen automatisch auf günstigere Speicherklassen umgestellt werden oder sie nach einem definierten Aufbewahrungszeitraum ablaufen. Weitere Informationen finden Sie unter Verwenden der S3-Versionierung mit S3 Lifecycle und Verwaltung des Lebenszyklus von Objekten.

Abhilfe

Informationen zur Verwendung der Versionierung in einem S3-Bucket finden Sie unter Aktivieren der Versionierung für Buckets im Amazon S3 S3-Benutzerhandbuch.

[S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0. 1/105.5.1, CRI-Profil v2. 2/DE. CM-09.01, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. DS-11.01

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-default-lock-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`mode`	Aufbewahrungsmodus von S3 Object Lock	Enum	`GOVERNANCE` , `COMPLIANCE`	Kein Standardwert

Dieses Steuerelement prüft, ob in einem Amazon S3 S3-Allzweck-Bucket Object Lock aktiviert ist. Die Steuerung schlägt fehl, wenn Object Lock für den Bucket nicht aktiviert ist. Wenn Sie einen

benutzerdefinierten Wert für den `mode` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn S3 Object Lock den angegebenen Aufbewahrungsmodus verwendet.

Mit der S3-Objektsperre können Sie Objekte anhand des Modells Write Once Read Many (WORM) speichern. Object Lock kann verhindern, dass Objekte in S3-Buckets für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben werden. Sie können die S3-Objektsperre verwenden, um regulatorische Anforderungen einzuhalten, die die WORM-Speicherung verlangen, oder um eine zusätzliche Schutzebene gegen Objektänderungen und -löschungen einzurichten.

Abhilfe

Informationen zur Konfiguration von Object Lock für neue und bestehende S3-Buckets finden Sie unter Konfiguration von S3 Object Lock im Amazon S3 S3-Benutzerhandbuch.

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Verwandte Anforderungen: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (10), (1), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11 NIST.800-53.r5 AU-9, 3.13.16, PCI DSS v4.0 NIST.800-171.r2. 1/35.5.1, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.07

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-default-encryption-kms

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon S3 S3-Allzweck-Bucket mit einem AWS KMS key (SSE-KMS oder DSSE-KMS) verschlüsselt ist. Die Kontrolle schlägt fehl, wenn der Bucket mit der Standardverschlüsselung (SSE-S3) verschlüsselt ist.

Server-side Verschlüsselung (SSE) ist die Verschlüsselung von Daten am Zielort durch die Anwendung oder den Dienst, der sie empfängt. Sofern Sie nichts anderes angeben, verwenden S3-Buckets standardmäßig von Amazon S3 verwaltete Schlüssel (SSE-S3) für die serverseitige Verschlüsselung. Für zusätzliche Kontrolle können Sie Buckets jedoch so konfigurieren, dass sie

stattdessen serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS oder) verwenden. DSSE-KMS Amazon S3 verschlüsselt Ihre Daten auf Objektebene, wenn es sie auf Festplatten in AWS Rechenzentren schreibt, und entschlüsselt sie für Sie, wenn Sie darauf zugreifen.

Abhilfe

Informationen zur Verschlüsselung eines S3-Buckets mit SSE-KMS finden Sie unter Serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) angeben im Amazon S3 S3-Benutzerhandbuch. Informationen zur Verschlüsselung eines S3-Buckets mit DSSE-KMS finden Sie unter Serverseitige Dual-Layer-Verschlüsselung mit AWS KMS keys (DSSE-KMS) angeben im Amazon S3 S3-Benutzerhandbuch.

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::AccessPoint`

AWS Config -Regel: s3-access-point-public-access-blocks

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für einen Amazon S3 S3-Zugriffspunkt die Einstellungen für den öffentlichen Zugriff blockiert aktiviert sind. Die Kontrolle schlägt fehl, wenn die Einstellungen zum Blockieren des öffentlichen Zugriffs für den Access Point nicht aktiviert sind.

Die Amazon S3 S3-Funktion Block Public Access hilft Ihnen, den Zugriff auf Ihre S3-Ressourcen auf drei Ebenen zu verwalten: Konto-, Bucket- und Access Point-Ebene. Die Einstellungen auf jeder Ebene können unabhängig voneinander konfiguriert werden, sodass Sie unterschiedliche Stufen der öffentlichen Zugriffsbeschränkungen für Ihre Daten festlegen können. Die Einstellungen des Access

Points können die restriktiveren Einstellungen auf höheren Ebenen (Kontoebene oder dem Access Point zugewiesener Bucket) nicht einzeln außer Kraft setzen. Stattdessen sind die Einstellungen auf der Zugriffspunktebene additiv, was bedeutet, dass sie die Einstellungen auf den anderen Ebenen ergänzen und mit ihnen zusammenarbeiten. Sofern Sie nicht beabsichtigen, dass ein S3-Zugriffspunkt öffentlich zugänglich ist, sollten Sie die Einstellungen zum Blockieren des öffentlichen Zugriffs aktivieren.

Abhilfe

Amazon S3 unterstützt derzeit nicht das Ändern der Public Block Access-Einstellungen eines Zugriffspunkts, nachdem der Zugriffspunkt erstellt wurde. Alle Einstellungen zum Blockieren des öffentlichen Zugriffs sind standardmäßig aktiviert, wenn Sie einen neuen Access Point erstellen. Wir empfehlen, alle Einstellungen aktiviert zu lassen, es sei denn, Sie wissen, dass Sie eine bestimmte Einstellung deaktivieren müssen. Weitere Informationen finden Sie unter Verwaltung des öffentlichen Zugriffs auf Access Points im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/21.1.2, Benchmark v3.0 für CIS AWS Foundations. 0/21.1.2, Benchmark für CIS AWS Foundations v1.4. 0/2.1.3, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CM-3, CRI-Profil v2. 2/PR. AA-03.01, CRI-Profil v2. 2/PR. AA-05.02, CRI-Profil v2. 2/PR. DS-01.01

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: s3-bucket-mfa-delete-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Löschen mit Multi-Faktor-Authentifizierung (MFA) für einen Amazon S3 S3-Allzweck-Bucket aktiviert ist. Die Steuerung schlägt fehl, wenn MFA Delete für den Bucket nicht aktiviert ist. Das Steuerelement liefert keine Ergebnisse für Buckets mit einer Lebenszykluskonfiguration.

Wenn Sie die Versionierung für einen S3-Allzweck-Bucket aktivieren, können Sie optional eine weitere Sicherheitsebene hinzufügen, indem Sie MFA Delete für den Bucket konfigurieren. In diesem

Fall muss der Bucket-Besitzer in jeder Anfrage zwei Arten der Authentifizierung angeben, um eine Version eines Objekts im Bucket zu löschen oder den Versionsstatus des Buckets zu ändern. MFA Delete bietet zusätzliche Sicherheit, wenn beispielsweise die Sicherheitsanmeldedaten des Bucket-Besitzers kompromittiert wurden. Das Löschen mit MFA kann auch dazu beitragen, versehentliches Löschen von Buckets zu verhindern, indem der Benutzer, der die Löschaktion initiiert, den physischen Besitz eines MFA-Geräts mit einem MFA-Code nachweisen muss, wodurch die Löschaktion noch reibungsloser und sicherer wird.

> **Note**
>
> Dieses Steuerelement erzeugt nur dann ein `PASSED` Ergebnis, wenn MFA Delete für den S3-Allzweck-Bucket aktiviert ist. Um MFA Delete für einen Bucket zu aktivieren, muss die Versionierung auch für den Bucket aktiviert sein. Die Bucket-Versionierung ist eine Methode zum Speichern mehrerer Varianten eines S3-Objekts im selben Bucket. Darüber hinaus kann nur der Bucket-Besitzer, der als Root-Benutzer angemeldet ist, das Löschen von MFA aktivieren und Löschaktionen für den Bucket ausführen. Sie können MFA Delete nicht mit einem Bucket verwenden, der über eine Lebenszykluskonfiguration verfügt.

Abhilfe

Informationen zur Aktivierung der Versionierung und zur Konfiguration von MFA Delete für einen S3-Bucket finden Sie unter MFA-Löschen konfigurieren im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.8, Benchmark v3.0 für CIS AWS Foundations. 0/3.8, PCI DSS v4.0. 1/10.2.1, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/PR. PS-04.02

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: cloudtrail-all-write-s3-data-event-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Schreibdatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle schlägt fehl, wenn das Konto nicht über einen Multi-Regions-Trail verfügt, der Schreibdatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject` `DeleteObject``PutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Schreibdatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt `PASSED` zu einem Ergebnis, wenn Sie einen Trail mit mehreren Regionen konfigurieren, der nur Schreibvorgänge oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v5.0. 0/3.9, Benchmark v3.0 für CIS AWS Foundations. 0/3.9, PCI DSS v4.0. 1/10.2.1, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. AE-07.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. AN-07.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: cloudtrail-all-read-s3-data-event-check

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Lesedatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle schlägt fehl, wenn das Konto nicht über einen Multiregions-Trail verfügt, der Lesedatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject` `DeleteObject``PutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Lesedatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt `PASSED` zu einem Ergebnis, wenn Sie einen Trail mit mehreren Regionen konfigurieren, der schreibgeschützte oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0. 1/14.4.4, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::S3::MultiRegionAccessPoint`

AWS Config Regel: `s3-mrap-public-access-blocked` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für einen Amazon S3 Multi-Region Access Point die Einstellungen für den öffentlichen Zugriff gesperrt sind. Die Kontrolle schlägt fehl, wenn für den Multi-Region Access Point die Einstellungen zum Sperren des öffentlichen Zugriffs nicht aktiviert sind.

Öffentlich zugängliche Ressourcen können zu unberechtigtem Zugriff, Datenschutzverletzungen oder der Ausnutzung von Sicherheitslücken führen. Die Einschränkung des Zugriffs durch Authentifizierungs- und Autorisierungsmaßnahmen trägt zum Schutz vertraulicher Informationen und zur Wahrung der Integrität Ihrer Ressourcen bei.

Abhilfe

Standardmäßig sind alle Block Public Access-Einstellungen für einen S3 Multi-Region Access Point aktiviert. Weitere Informationen finden Sie unter Blockieren des öffentlichen Zugriffs mit Amazon S3 Multi-Region Access Points im Amazon Simple Storage Service-Benutzerhandbuch. Sie können die Einstellungen zum Sperren des öffentlichen Zugriffs für einen Multi-Region Access Point nicht mehr ändern, nachdem er erstellt wurde.

[S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

Kategorie: Schützen > Datenschutz

Schweregrad: Niedrig

Art der Ressource: `AWS::S3Express::DirectoryBucket`

AWS Config -Regel: s3express-dir-bucket-lifecycle-rules-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`targetExpirationDays`	Die Anzahl der Tage nach der Objekterstellung, an denen Objekte ablaufen sollen.	Ganzzahl	1 auf 2147483647	Kein Standardwert

Dieses Steuerelement prüft, ob Lebenszyklusregeln für einen S3-Verzeichnis-Bucket konfiguriert sind. Die Steuerung schlägt fehl, wenn keine Lebenszyklusregeln für den Directory-Bucket konfiguriert sind oder eine Lebenszyklusregel für den Bucket Ablaufeinstellungen festlegt, die nicht mit dem Parameterwert übereinstimmen, den Sie optional angeben.

In Amazon S3 besteht eine Lebenszykluskonfiguration aus einer Reihe von Regeln, die Aktionen definieren, die Amazon S3 auf eine Gruppe von Objekten in einem Bucket anwenden soll. Für einen S3-Verzeichnis-Bucket können Sie eine Lebenszyklusregel erstellen, die je nach Alter (in Tagen) festlegt, wann Objekte ablaufen. Sie können auch eine Lebenszyklusregel erstellen, die unvollständige mehrteilige Uploads löscht. Im Gegensatz zu anderen Arten von S3-Buckets, wie z. B. Allzweck-Buckets, unterstützen Directory-Buckets keine anderen Arten von Aktionen für Lebenszyklusregeln, wie z. B. den Übergang von Objekten zwischen Speicherklassen.

Abhilfe

Um eine Lebenszykluskonfiguration für einen S3-Verzeichnis-Bucket zu definieren, erstellen Sie eine Lebenszyklusregel für den Bucket. Weitere Informationen finden Sie unter Erstellen und Verwalten einer Lebenszykluskonfiguration für Ihren Directory-Bucket im Amazon Simple Storage Service-Benutzerhandbuch.

Security Hub CSPM-Steuerungen für KI SageMaker

Diese AWS Security Hub CSPM Kontrollen bewerten den Amazon SageMaker AI-Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: sagemaker-notebook-no-direct-internet-access

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der direkte Internetzugang für eine SageMaker AI-Notebook-Instanz deaktiviert ist. Die Steuerung schlägt fehl, wenn das `DirectInternetAccess` Feld für die Notebook-Instanz aktiviert ist.

Wenn Sie Ihre SageMaker AI-Instance ohne VPC konfigurieren, ist der direkte Internetzugang auf Ihrer Instance standardmäßig aktiviert. Sie sollten Ihre Instance mit einer VPC konfigurieren und die Standardeinstellung auf Deaktivieren — Zugriff auf das Internet über eine VPC ändern. Um Modelle von einem Notebook aus zu trainieren oder zu hosten, benötigen Sie Internetzugang. Um den Internetzugang zu aktivieren, muss Ihre VPC entweder über einen Schnittstellenendpunkt (AWS PrivateLink) oder ein NAT-Gateway und eine Sicherheitsgruppe verfügen, die ausgehende Verbindungen zulässt. Weitere Informationen zum Connect einer Notebook-Instance mit Ressourcen in einer VPC finden Sie unter Verbinden einer Notebook-Instance mit Ressourcen in einer VPC im Amazon SageMaker AI Developer Guide. Sie sollten auch sicherstellen, dass der Zugriff auf Ihre SageMaker KI-Konfiguration nur auf autorisierte Benutzer beschränkt ist. Schränken Sie IAM-Berechtigungen ein, die es Benutzern ermöglichen, SageMaker KI-Einstellungen und -Ressourcen zu ändern.

Abhilfe

Sie können die Internetzugriffseinstellungen nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz mit blockiertem Internetzugang beenden, löschen und neu erstellen. Informationen zum Löschen einer Notebook-Instance, die direkten Internetzugang ermöglicht, finden Sie unter Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen im Amazon SageMaker AI Developer Guide. Informationen zum Neuerstellen einer Notebook-Instance, die den Internetzugang verweigert, finden Sie unter Notebook-Instance erstellen. Wählen Sie für Netzwerk, Direkter Internetzugang die Option Deaktivieren — Zugriff auf das Internet über eine VPC.

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7,

NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), CRI Profile v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: sagemaker-notebook-instance-inside-vpc

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon SageMaker AI-Notebook-Instance in einer benutzerdefinierten Virtual Private Cloud (VPC) gestartet wird. Diese Steuerung schlägt fehl, wenn eine SageMaker KI-Notebook-Instance nicht in einer benutzerdefinierten VPC oder in der SageMaker AI-Service-VPC gestartet wird.

Subnetze sind ein Bereich von IP-Adressen innerhalb einer VPC. Wir empfehlen, Ihre Ressourcen wann immer möglich in einer benutzerdefinierten VPC aufzubewahren, um einen sicheren Netzwerkschutz Ihrer Infrastruktur zu gewährleisten. Eine Amazon VPC ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Mit einer Amazon VPC können Sie den Netzwerkzugriff und die Internetverbindung Ihrer SageMaker AI Studio- und Notebook-Instances steuern.

Abhilfe

Sie können die VPC-Einstellung nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz beenden, löschen und neu erstellen. Anweisungen finden Sie unter Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen im Amazon SageMaker AI Developer Guide.

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2), CRI Profile v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. AA-05.02

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: sagemaker-notebook-instance-root-access-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Zugriff für eine Amazon SageMaker AI-Notebook-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn der Root-Zugriff für eine SageMaker AI-Notebook-Instance aktiviert ist.

Unter Einhaltung des Prinzips der geringsten Rechte wird empfohlen, den Root-Zugriff auf Instanzressourcen zu beschränken, um eine unbeabsichtigte Überzuweisung von Zugriffsberechtigungen zu vermeiden.

Abhilfe

Informationen zum Einschränken des Root-Zugriffs auf SageMaker KI-Notebook-Instances finden Sie unter Steuern des Root-Zugriffs auf eine SageMaker KI-Notebook-Instance im Amazon SageMaker AI Developer Guide.

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36 NIST.800-53.r5 SA-13, CRI Profile v2. 2/PR. IR-03.01, CRI-Profil v2. 2/PR. IR-04.02

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::EndpointConfig`

AWS Config -Regel: sagemaker-endpoint-config-prod-instance-count

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Produktionsvarianten eines Amazon SageMaker AI-Endpunkts eine anfängliche Instanzzahl von mehr als 1 aufweisen. Die Kontrolle schlägt fehl, wenn die Produktionsvarianten des Endpunkts nur eine erste Instanz haben.

Produktionsvarianten, die mit einer Instanzzahl von mehr als 1 ausgeführt werden, ermöglichen Multi-AZ-Instance-Redundanz, die von KI verwaltet wirdSageMaker . Die Bereitstellung von Ressourcen in mehreren Availability Zones ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur zu gewährleisten. Hochverfügbarkeit hilft Ihnen, sich nach Sicherheitsvorfällen zu erholen.

> **Note**
>
> Diese Steuerung gilt nur für die instanzbasierte Endpunktkonfiguration.

Abhilfe

Weitere Informationen zu den Parametern der Endpunktkonfiguration finden Sie unter Erstellen einer Endpunktkonfiguration im Amazon SageMaker AI Developer Guide.

[SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::Model`

AWS Config -Regel: sagemaker-model-isolation-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob bei einem von Amazon SageMaker AI gehosteten Modell die Netzwerkisolierung aktiviert ist. Die Steuerung schlägt fehl, wenn der `EnableNetworkIsolation` Parameter für das gehostete Modell auf gesetzt ist`False`.

SageMaker KI-Training und bereitgestellte Inferenzcontainer sind standardmäßig internetfähig. Wenn Sie nicht möchten, dass SageMaker KI externen Netzwerkzugriff auf Ihre Trainings- oder Inferenzcontainer gewährt, können Sie die Netzwerkisolierung aktivieren. Wenn Sie die Netzwerkisolierung aktivieren, können keine eingehenden oder ausgehenden Netzwerkanrufe an oder von dem Modellcontainer getätigt werden, auch keine Aufrufe an oder von anderen. AWS-Services Darüber hinaus werden der Container-Laufzeitumgebung keine AWS Anmeldeinformationen zur Verfügung gestellt. Durch die Aktivierung der Netzwerkisolierung wird ein unbeabsichtigter Zugriff auf Ihre SageMaker KI-Ressourcen aus dem Internet verhindert.

> **Note**
>
> Am 13. August 2025 änderte Security Hub CSPM den Titel und die Beschreibung dieses Steuerelements. Der neue Titel und die neue Beschreibung geben genauer wieder, dass das Steuerelement die Einstellung für den `EnableNetworkIsolation` Parameter der von Amazon SageMaker AI gehosteten Modelle überprüft. Zuvor lautete der Titel dieses Steuerelements: SageMaker models should block inbound traffic.

Abhilfe

Weitere Informationen zur Netzwerkisolierung für SageMaker KI-Modelle finden Sie unter Ausführen von Trainings- und Inferenzcontainern im internetfreien Modus im Amazon SageMaker AI Developer Guide. Wenn Sie ein Modell erstellen, können Sie die Netzwerkisolierung aktivieren, indem Sie den Wert für den `EnableNetworkIsolation` Parameter auf setzen. `True`

[SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SageMaker::AppImageConfig`

AWS Config -Regel: sagemaker-app-image-config-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon SageMaker AI-App-Image-Konfiguration (`AppImageConfig`) die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Konfiguration des App-Images keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die App-Image-Konfiguration keine Tag-Schlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einer Amazon SageMaker AI-App-Image-Konfiguration (`AppImageConfig`) Tags hinzuzufügen, können Sie den AddTagsBetrieb der SageMaker KI-API verwenden oder, falls Sie die verwenden AWS CLI, den Befehl add-tags ausführen.

[SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Taggen

Schweregrad: Niedrig

Art der Ressource: `AWS::SageMaker::Image`

AWS Config -Regel: sagemaker-image-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon SageMaker AI-Image die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel hat. Die Steuerung schlägt fehl, wenn das Bild keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Bild keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einem Amazon SageMaker AI-Image Tags hinzuzufügen, können Sie den AddTagsBetrieb der SageMaker AI-API verwenden oder, falls Sie die verwenden AWS CLI, den Befehl add-tags ausführen.

[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen

Verwandte Anforderungen: CRI Profile v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-02.02

Kategorie: Erkennen > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: sagemaker-notebook-instance-platform-version

Art des Zeitplans: Periodisch

Parameter:

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1` (nicht anpassbar)

Dieses Steuerelement prüft anhand der für die Notebook-Instance angegebenen Plattform-ID, ob eine Amazon SageMaker AI-Notebook-Instance für die Ausführung auf einer unterstützten Plattform konfiguriert ist. Die Steuerung schlägt fehl, wenn die Notebook-Instance für die Ausführung auf einer Plattform konfiguriert ist, die nicht mehr unterstützt wird.

Wenn die Plattform für eine Amazon SageMaker AI-Notebook-Instance nicht mehr unterstützt wird, erhält sie möglicherweise keine Sicherheitspatches, Bugfixes oder andere Arten von Updates. Notebook-Instances funktionieren möglicherweise weiterhin, erhalten jedoch keine SageMaker KI-Sicherheitsupdates oder kritische Bugfixes. Sie übernehmen die Risiken, die mit der Verwendung einer nicht unterstützten Plattform verbunden sind. Weitere Informationen finden Sie unter JupyterLabVersionierung im Amazon SageMaker AI Developer Guide.

Abhilfe

Informationen zu den Plattformen, die Amazon SageMaker AI derzeit unterstützt, und zur Migration zu diesen Plattformen finden Sie unter Amazon Linux 2-Notebook-Instances im Amazon SageMaker AI Developer Guide.

[SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::DataQualityJobDefinition`

AWS Config -Regel: sagemaker-data-quality-job-encrypt-in-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon SageMaker AI-Auftragsdefinition zur Datenqualität die Verschlüsselung für den Verkehr zwischen Containern aktiviert ist. Die Kontrolle schlägt fehl, wenn in der Definition für einen Job, der Datenqualität und Datendrift überwacht, die Verschlüsselung für den Verkehr zwischen Containern nicht aktiviert ist.

Durch die Aktivierung der Verschlüsselung des Datenverkehrs zwischen Containern werden sensible ML-Daten während der verteilten Verarbeitung zur Datenqualitätsanalyse geschützt.

Abhilfe

Weitere Informationen zur Verschlüsselung des Datenverkehrs zwischen Containern für Amazon SageMaker AI finden Sie unter Schützen der Kommunikation zwischen ML-Compute-Instances in a Distributed Training Job im Amazon SageMaker AI Developer Guide. Wenn Sie eine Auftragsdefinition für die Datenqualität erstellen, können Sie die Verschlüsselung des Datenverkehrs zwischen Containern aktivieren, indem Sie den Wert für den `EnableInterContainerTrafficEncryption` Parameter auf festlegen. `True`

Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config -Regel: sagemaker-model-explainability-job-encrypt-in-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einer Auftragsdefinition für Erklärbarkeit im SageMaker Amazon-Modell die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert ist. Die Kontrolle schlägt fehl, wenn in der Auftragsdefinition für die Erklärung des Modells die Verschlüsselung des Datenverkehrs zwischen Containern nicht aktiviert ist.

Durch die Aktivierung der Verschlüsselung des Datenverkehrs zwischen Containern werden sensible ML-Daten wie Modelldaten, Trainingsdatensätze, Zwischenverarbeitungsergebnisse, Parameter und Modellgewichte während der verteilten Verarbeitung zur Erklärbarkeitsanalyse geschützt.

Abhilfe

Bei einer bestehenden Aufgabendefinition zur Erläuterung von SageMaker Modellen kann die Verschlüsselung des Datenverkehrs zwischen Containern nicht an Ort und Stelle aktualisiert werden. Verwenden Sie API oder CLI oder und stellen Sie auf ein, um eine neue Jobdefinition zur Erläuterung des SageMaker Modells mit aktivierter Verschlüsselung für den Containerverkehr zu erstellen. `CloudFormationEnableInterContainerTrafficEncryption``True`

[SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Ressourcentyp: `AWS::SageMaker::DataQualityJobDefinition`

AWS Config -Regel: sagemaker-data-quality-job-isolation

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Auftragsdefinition zur Überwachung der Datenqualität von Amazon SageMaker AI die Netzwerkisolierung aktiviert ist. Die Steuerung schlägt fehl, wenn in der Definition für einen Job, der Datenqualität und -drift überwacht, die Netzwerkisolierung deaktiviert ist.

Die Netzwerkisolierung reduziert die Angriffsfläche und verhindert externen Zugriff, wodurch vor unbefugtem Zugriff von außen, versehentlicher Datenoffenlegung und potenzieller Datenexfiltration geschützt wird.

Abhilfe

Weitere Informationen zur Netzwerkisolierung für SageMaker KI finden Sie unter Ausführen von Trainings- und Inferenzcontainern im internetfreien Modus im Amazon SageMaker AI Developer Guide. Wenn Sie eine Auftragsdefinition für Datenqualität erstellen, können Sie die Netzwerkisolierung aktivieren, indem Sie den Wert für den `EnableNetworkIsolation` Parameter auf setzen. `True`

Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Konfiguration der Ressourcenrichtlinie

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::ModelBiasJobDefinition`

AWS Config -Regel: sagemaker-model-bias-job-isolation

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei einer Jobdefinition mit SageMaker Modellverzerrung die Netzwerkisolierung aktiviert ist. Die Steuerung schlägt fehl, wenn bei der Jobdefinition für Modellverzerrungen die Netzwerkisolierung nicht aktiviert ist.

Die Netzwerkisolierung verhindert, dass SageMaker Model-Bass-Jobs über das Internet mit externen Ressourcen kommunizieren. Durch die Aktivierung der Netzwerkisolierung stellen Sie sicher, dass die Container des Auftrags keine ausgehenden Verbindungen herstellen können. Dadurch wird die Angriffsfläche reduziert und sensible Daten werden vor dem Eindringen geschützt. Dies ist besonders wichtig für Jobs, die regulierte oder sensible Daten verarbeiten.

Abhilfe

Um die Netzwerkisolierung zu aktivieren, müssen Sie eine neue Model Bias-Jobdefinition erstellen, bei der der `EnableNetworkIsolation` Parameter auf gesetzt ist`True`. Die Netzwerkisolierung kann nach der Erstellung der Auftragsdefinition nicht geändert werden. Informationen zur Erstellung einer neuen Model Bias-Jobdefinition finden Sie CreateModelBiasJobDefinitionim Amazon SageMaker AI Developer Guide.

[SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config -Regel: ssagemaker-model-quality-job-encrypt-in-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei Auftragsdefinitionen von Amazon SageMaker Model Quality die Verschlüsselung während der Übertragung für den Verkehr zwischen Containern aktiviert ist. Die Kontrolle schlägt fehl, wenn in einer Auftragsdefinition in Modellqualität die Verschlüsselung des Datenverkehrs zwischen Containern nicht aktiviert ist.

Inter-container Die Datenverkehrsverschlüsselung schützt Daten, die während verteilter Aufgaben zur Überwachung der Modellqualität zwischen Containern übertragen werden. Standardmäßig ist der Verkehr zwischen Containern unverschlüsselt. Die Aktivierung der Verschlüsselung trägt zur Wahrung der Datenvertraulichkeit bei der Verarbeitung bei und unterstützt die Einhaltung der gesetzlichen Anforderungen für den Schutz von Daten bei der Übertragung.

Abhilfe

Um die Verschlüsselung des intercontainerübergreifenden Datenverkehrs für Ihre Auftragsdefinition in SageMaker Amazon-Modellqualität zu aktivieren, müssen Sie die Auftragsdefinition mit der entsprechenden Verschlüsselungskonfiguration während der Übertragung neu erstellen. Informationen zur Erstellung einer Jobdefinition in Modellqualität finden Sie CreateModelQualityJobDefinitionim Amazon SageMaker AI Developer Guide.

[SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Ressourcentyp: `AWS::SageMaker::MonitoringSchedule`

AWS Config -Regel: sagemaker-monitoring-schedule-isolation

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Netzwerkisolierung in den SageMaker Amazon-Überwachungsplänen aktiviert ist. Die Steuerung schlägt fehl, wenn ein Überwachungsplan auf „Falsch“ EnableNetworkIsolation gesetzt oder nicht konfiguriert wurde

Die Netzwerkisolierung verhindert, dass Überwachungsaufträge ausgehende Netzwerkanrufe tätigen, wodurch die Angriffsfläche reduziert wird, da der Internetzugang aus Containern ausgeschlossen wird.

Abhilfe

Informationen zur Konfiguration der Netzwerkisolierung im NetworkConfig Parameter bei der Erstellung oder Aktualisierung eines Überwachungsplans finden Sie unter CreateMonitoringScheduleoder UpdateMonitoringScheduleim Amazon SageMaker AI Developer Guide.

[SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::ModelBiasJobDefinition`

AWS Config -Regel: sagemaker-model-bias-job-encrypt-in-transit

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei Auftragsdefinitionen mit Amazon SageMaker Model Bias die Verschlüsselung des intercontainerübergreifenden Datenverkehrs aktiviert ist, wenn mehrere Compute-Instances verwendet werden. Die Steuerung schlägt fehl, wenn sie `EnableInterContainerTrafficEncryption` auf „Falsch“ gesetzt oder nicht für Jobdefinitionen mit einer Instance-Anzahl von 2 oder mehr konfiguriert ist.

Inter-container Die Verschlüsselung des Datenverkehrs schützt Daten, die zwischen Recheninstanzen während der Überwachung verteilter Modellfehler übertragen werden. Die Verschlüsselung verhindert den unbefugten Zugriff auf modellbezogene Informationen wie Gewichte, die zwischen Instanzen übertragen werden.

Abhilfe

Um die Verschlüsselung des Datenverkehrs zwischen Containern für SageMaker Model-Basis-Jobdefinitionen zu aktivieren, setzen Sie den `EnableInterContainerTrafficEncryption` Parameter auf, `True` wenn die Auftragsdefinition mehrere Recheninstanzen verwendet. Informationen zum Schutz der Kommunikation zwischen ML-Compute-Instances finden Sie unter Schützen der Kommunikation zwischen ML-Compute-Instances in a Distributed Training Job im Amazon SageMaker AI Developer Guide.

[SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::Model`

AWS Config -Regel: sagemaker-model-private-registry-required

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon SageMaker AI-Modell ein Container-Image aus einer privaten Registrierung in einer VPC für den primären Container abruft. Die Steuerung schlägt fehl, wenn das Image nicht konfiguriert ist oder der Repository-Zugriffsmodus aktiviert ist. `Platform`

Durch die Verwendung einer privaten Docker-Registry in einer VPC für SageMaker Modellcontainer wird sichergestellt, dass Container-Images aus vertrauenswürdigen, kontrollierten Quellen innerhalb Ihrer VPC abgerufen werden. Außerdem wird sichergestellt, dass auf Container-Images über VPC-Endpunkte zugegriffen wird, ohne das öffentliche Internet zu durchqueren.

Abhilfe

Informationen zur Konfiguration privater Docker-Registrierungen für SageMaker KI-Echtzeit-Inferenzcontainer finden Sie unter Verwenden einer privaten Docker-Registrierung für Real-Time Inferenzcontainer im Amazon AI Developer Guide. SageMaker

[SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::FeatureGroup`

AWS Config -Regel: sagemaker-featuregroup-encryption-at-rest

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein SageMaker Amazon-Offline-Shop für eine Feature-Gruppe im Ruhezustand mit einem AWS KMS Schlüssel verschlüsselt ist. Die Steuerung schlägt fehl, wenn der S3-Speicher des Offline-Speichers für eine Feature-Gruppe nicht mit einem KMS-Schlüssel verschlüsselt ist.

Die Verwendung der vom Kunden AWS KMS keys verwalteten Verschlüsselung in den Offline-Stores der restlichen SageMaker Featuregruppe bietet mehr Sicherheit. Customer-managed Mit KMS-Schlüsseln haben Sie die volle Kontrolle über den Lebenszyklus und die Schlüsselrichtlinien von Verschlüsselungsschlüsseln. Darüber hinaus kann die gesamte Verwendung von Verschlüsselungsschlüsseln protokolliert und aus AWS CloudTrail Gründen der Überprüfbarkeit überwacht werden.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für SageMaker Feature Store-Offline-Shops, die AWS KMS vom Kunden verwaltete Schlüssel verwenden, finden Sie unter Sicherheit und Zugriffskontrolle im Amazon SageMaker AI Developer Guide.

[SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::FeatureGroup`

AWS Config -Regel: sagemaker-featuregroup-online-store-encryption

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein SageMaker Amazon-Onlineshop für eine Feature-Gruppe mit Standardspeicher im Ruhezustand mit einem AWS KMS Schlüssel verschlüsselt ist. Die Steuerung schlägt fehl, wenn die KMS-Schlüsselverschlüsselung nicht für den Online-Shop konfiguriert ist.

Die vom Kunden AWS KMS keys verwaltete Verschlüsselung in Onlineshops mit anderen SageMaker Featuregruppen bietet mehr Sicherheit. Customer-managed Mit KMS-Schlüsseln haben Sie die volle Kontrolle über den Lebenszyklus und die Schlüsselrichtlinien von Verschlüsselungsschlüsseln. Darüber hinaus kann die gesamte Verwendung von Verschlüsselungsschlüsseln protokolliert und aus AWS CloudTrail Gründen der Überprüfbarkeit überwacht werden.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für SageMaker Feature Store-Onlineshops, die AWS KMS vom Kunden verwaltete Schlüssel verwenden, finden Sie unter Sicherheit und Zugriffskontrolle im Amazon SageMaker AI Developer Guide.

[SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::Model`

AWS Config -Regel: sagemaker-model-multicontainer-private-registry

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon SageMaker AI-Modelle mit Inferenz-Pipelines für mehrere Container Container-Images aus einer privaten Docker-Registry in einer VPC abrufen. Die Steuerung schlägt fehl, wenn für eine Container-Definition keine Image-Konfiguration oder der Repository-Zugriffsmodus auf Plattform gesetzt ist.

Durch die Verwendung einer privaten Docker-Registry in einer VPC für SageMaker KI-Inferenz-Pipelines mit mehreren Containern wird sichergestellt, dass Container-Images aus vertrauenswürdigen, kontrollierten Quellen innerhalb Ihrer VPC abgerufen werden. Dadurch wird sichergestellt, dass auf Container-Images über VPC-Endpunkte zugegriffen wird, ohne das öffentliche Internet zu durchqueren, wodurch das Risiko von Supply-Chain-Angriffen oder Image-Manipulationen reduziert wird.

Abhilfe

Informationen zur Konfiguration privater Docker-Registrierungen für SageMaker KI-Echtzeit-Inferenzcontainer finden Sie unter Verwenden einer privaten Docker-Registrierung für Real-Time Inferenzcontainer im Amazon AI Developer Guide. SageMaker

[SageMaker.20] Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells sollte die Netzwerkisolierung aktiviert sein

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config -Regel: sagemaker-model-explainability-job-network-isolation

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Jobdefinition zur Erklärbarkeit eines SageMaker KI-Modells die Netzwerkisolierung aktiviert ist. Die Steuerung schlägt fehl, wenn in der Auftragsdefinition die Netzwerkisolierung nicht aktiviert ist.

Die Netzwerkisolierung verhindert, dass Jobcontainer mit Modellerklärbarkeit ausgehende Netzwerkaufrufe tätigen, wodurch das Risiko einer Datenexfiltration reduziert wird und ein umfassender Schutz für sensible Modell- und Trainingsdaten gewährleistet wird.

Abhilfe

Um die Netzwerkisolierung für eine Jobdefinition zur Erklärbarkeit eines SageMaker KI-Modells zu aktivieren, stellen Sie bei der Erstellung der Jobdefinition die Option auf ein. `NetworkConfig.EnableNetworkIsolation` `true` Weitere Informationen zur Netzwerkisolierung für SageMaker KI finden Sie unter Ausführen von Trainings- und Inferenzcontainern im internetfreien Modus im Amazon SageMaker AI Developer Guide.

[SageMaker.21] SageMaker Notebook-Instances sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Ressourcentyp: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: sagemaker-notebook-instance-storage-vol-kms-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine SageMaker KI-Notebook-Instanz mit einem AWS KMS Schlüssel für die Verschlüsselung von Speichervolumes konfiguriert ist. Die Steuerung schlägt fehl, wenn kein KMS-Schlüssel für die Notebook-Instanz konfiguriert ist.

Die Verschlüsselung ruhender Daten mit einem vom Kunden verwalteten KMS-Schlüssel bietet zusätzliche Zugriffskontrolle gegenüber der standardmäßigen AWS verwalteten Verschlüsselung. SageMaker KI-Notebook-Instances speichern Benutzernotizbücher, Datensätze, Modellartefakte und temporäre Verarbeitungsdaten auf ML-Speichervolumes. Ein vom Kunden verwalteter Schlüssel ermöglicht eine detaillierte Steuerung der Schlüsselrichtlinien, die CloudTrail Protokollierung der Schlüsselnutzung und die Einhaltung von Frameworks, die eine vom Kunden kontrollierte Verschlüsselung erfordern.

Abhilfe

Informationen zur Konfiguration eines KMS-Schlüssels für eine SageMaker KI-Notebook-Instance finden Sie unter Notebook-Instances, SageMaker AI-Jobs und Endpoints im Amazon SageMaker AI Developer Guide. Beachten `KmsKeyId` Sie, dass dies nur bei der Erstellung der Notebook-Instance festgelegt werden kann. Um das Problem zu beheben, erstellen Sie eine neue Notebook-Instanz mit dem angegebenen KMS-Schlüssel und migrieren Sie Ihre Daten aus der vorhandenen Instanz.

[SageMaker.22] In den SageMaker Überwachungsplänen sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Ressourcentyp: `AWS::SageMaker::MonitoringSchedule`

AWS Config -Regel: sagemaker-monitoring-schedule-traffic-encryption

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob in einem Amazon SageMaker AI-Überwachungsplan die Verschlüsselung für den Verkehr zwischen Containern aktiviert ist. Die Kontrolle schlägt fehl, wenn in der Definition des Überwachungsauftrags die Verschlüsselung für den Verkehr zwischen Containern nicht aktiviert ist.

Inter-container Die Datenverkehrsverschlüsselung stellt sicher, dass Daten, die während der Überwachung von Jobs zwischen Containern übertragen werden, während der Übertragung verschlüsselt werden. Ohne diese Verschlüsselung könnten sensible Daten, die während der Modellüberwachung verarbeitet werden, innerhalb des Netzwerks unbefugten Zugriffen ausgesetzt sein. Die Aktivierung dieser Einstellung trägt dazu bei, die Compliance-Anforderungen zum Schutz von Daten während der Übertragung zu erfüllen.

Abhilfe

Bei einem bestehenden SageMaker KI-Überwachungsplan kann die Verschlüsselung des Datenverkehrs zwischen Containern nicht aktualisiert werden. Um einen neuen SageMaker KI-Überwachungsplan mit aktivierter Verschlüsselung des Datenverkehrs zwischen Containern zu erstellen, verwenden Sie API oder CLI oder CloudFormation und setzen `EnableInterContainerTrafficEncryption` Sie `true` in der `NetworkConfig` `MonitoringJobDefinition` von auf.

[SageMaker.23] Bei SageMaker Inferenzexperimenten sollte das Instanz-Speichervolumen verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::InferenceExperiment`

AWS Config -Regel: sagemaker-inf-experiment-instance-storage-kms-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein SageMaker KI-Inferenzexperiment mit einem AWS KMS Schlüssel konfiguriert ist, z. B. mit der Verschlüsselung von Speichervolumes. Die Steuerung schlägt

fehl, wenn kein KMS-Schlüssel für die Verschlüsselung von Instance-Speichervolumes angegeben ist.

Die Verschlüsselung von Instance-Speichervolumes mit vom Kunden verwalteten KMS-Schlüsseln ermöglicht eine zentrale Schlüsselverwaltung, Auditprotokollierung und Steuerung der Schlüsselrotation für Modellartefakte und temporäre Inferenzdaten, die während Shadow-Tests auf ML-Compute-Instances gespeichert werden.

Abhilfe

Um einen KMS-Schlüssel für ein SageMaker KI-Inferenzexperiment zu konfigurieren, geben Sie den `KmsKey` Parameter beim Aufrufen an. `CreateInferenceExperiment` Dabei `KmsKey` kann es sich um eine KMS-Schlüssel-ID, einen ARN, einen Alias oder einen Alias-ARN ARN. Die SageMaker AI-Ausführungsrolle muss über `kms:CreateGrant` Berechtigungen für den Schlüssel verfügen. Weitere Informationen zur Angabe eines kundenverwalteten AWS KMS Schlüssels für SageMaker KI finden Sie unter Notebook-Instances, SageMaker KI-Jobs und Endpoints im Amazon SageMaker AI Developer Guide.

[SageMaker.24] Bei SageMaker Inferenzexperimenten sollte der Datenspeicher verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::InferenceExperiment`

AWS Config -Regel: sagemaker-inf-experiment-data-storage-kms-encrypted

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein SageMaker KI-Inferenzexperiment mit aktivierter Datenerfassung über einen KMS-Schlüssel verfügt, der so konfiguriert ist, dass erfasste Daten im Ruhezustand verschlüsselt werden. Die Steuerung schlägt fehl, wenn in der Datenspeicherkonfiguration kein KMS-Schlüssel für die Verschlüsselung angegeben ist.

Durch die Verschlüsselung erfasster Inferenzanforderungs- und Antwortdaten mit vom Kunden verwalteten KMS-Schlüsseln wird sichergestellt, dass sensible Inferenz-Payloads, die in Amazon S3 gespeichert sind, durch zentrale Schlüsselverwaltungs- und Prüffunktionen geschützt sind.

Abhilfe

Um einen KMS-Schlüssel für die Datenspeicherung in einem SageMaker KI-Inferenzexperiment zu konfigurieren, geben Sie beim Aufrufen das `KmsKey` darin enthaltene Feld an. `DataStorageConfig` `CreateInferenceExperiment` Das `KmsKey` verschlüsselt die erfassten Inferenzanforderungs- und Antwortdaten, die sich im angegebenen Amazon S3 S3-Bucket befinden. Weitere Informationen zur Angabe eines kundenverwalteten AWS KMS Schlüssels für SageMaker KI finden Sie unter Notebook-Instances, SageMaker KI-Jobs und Endpoints im Amazon SageMaker AI Developer Guide.

[SageMaker.25] Bei Jobdefinitionen in SageMaker Modellqualität sollte die Netzwerkisolierung aktiviert sein

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config -Regel: sagemaker-model-quality-job-definition-isolation

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei einer Jobdefinition für die Qualität eines Amazon SageMaker AI-Modells die Netzwerkisolierung aktiviert ist. Die Kontrolle schlägt fehl, wenn in der Auftragsdefinition für Modellqualität die Netzwerkisolierung nicht aktiviert ist.

Die Netzwerkisolierung reduziert die Angriffsfläche und verhindert externen Zugriff, wodurch vor unbefugtem Zugriff von außen, versehentlicher Datenoffenlegung und potenzieller Datenexfiltration geschützt wird.

Abhilfe

Wenn Sie eine Jobdefinition für Modellqualität erstellen, können Sie die Netzwerkisolierung aktivieren, indem Sie den Wert für den `EnableNetworkIsolation` Parameter auf `True` setzen. Weitere Informationen zur Netzwerkisolierung für SageMaker KI finden Sie unter Ausführen von Trainings- und Inferenzcontainern im internetfreien Modus im Amazon SageMaker AI Developer Guide.

Security Hub CSPM-Steuerelemente für Secrets Manager

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Secrets Manager Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.6.3, PCI DSS v4.0. 1/8.3.9, CRI-Profil v2. 2/PR. AA-01.01

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-rotation-enabled-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`maximumAllowedRotationFrequency`	Höchstzulässige Anzahl von Tagen für die geheime Rotationsfrequenz	Ganzzahl	1 auf 365	Kein Standardwert

Dieses Steuerelement prüft, ob ein in gespeichertes Geheimnis mit automatischer Rotation konfiguriert AWS Secrets Manager ist. Die Steuerung schlägt fehl, wenn das Geheimnis nicht mit automatischer Rotation konfiguriert ist. Wenn Sie einen benutzerdefinierten Wert für den

`maximumAllowedRotationFrequency` Parameter angeben, ist die Kontrolle nur erfolgreich, wenn das Geheimnis innerhalb des angegebenen Zeitfensters automatisch rotiert wird.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Secrets zentral zu speichern, Secrets automatisch zu verschlüsseln, den Zugriff auf Secrets zu kontrollieren und Secrets sicher und automatisch zu rotieren.

Secrets Manager kann Geheimnisse rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln. Weitere Informationen zur Rotation findest du unter Rotation deiner AWS Secrets Manager Geheimnisse im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.6.3, PCI DSS v4.0. 1/8.3.9, CRI-Profil v2. 2/PR. AA-01.01

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-scheduled-rotation-success-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft anhand des Rotationsplans, ob ein AWS Secrets Manager Secret erfolgreich rotiert wurde. Wenn `RotationOccurringAsScheduled` ja, schlägt die Steuerung fehl`false`. Das Steuerelement wertet nur Geheimnisse aus, bei denen die Rotation aktiviert ist.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Secrets zentral zu speichern, Secrets automatisch zu verschlüsseln, den Zugriff auf Secrets zu kontrollieren und Secrets sicher und automatisch zu rotieren.

Secrets Manager kann Geheimnisse rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln.

Zusätzlich zur Konfiguration der automatischen Rotation sollten Sie sicherstellen, dass diese Secrets gemäß dem Rotationsplan erfolgreich rotiert werden.

Weitere Informationen zur Rotation finden Sie unter Rotation Ihrer AWS Secrets Manager Geheimnisse im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Wenn die automatische Rotation fehlschlägt, sind bei Secrets Manager möglicherweise Fehler bei der Konfiguration aufgetreten. Um Secrets in Secrets Manager zu rotieren, verwenden Sie eine Lambda-Funktion, die definiert, wie mit der Datenbank oder dem Dienst, dem das Geheimnis gehört, interagiert werden soll.

Hilfe zur Diagnose und Behebung häufiger Fehler im Zusammenhang mit der Rotation von Geheimnissen finden Sie unter Fehlerbehebung bei der AWS Secrets Manager Rotation von Geheimnissen im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), CRI-Profil v2. 2/PR. AA-01.01, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. AA-05.03

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-secret-unused`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`unusedForDays`	Maximale Anzahl von Tagen, an denen ein Geheimnis ungenutzt bleiben kann	Ganzzahl	1 auf 365	90

Dieses Steuerelement prüft, ob innerhalb des angegebenen Zeitraums auf ein AWS Secrets Manager Geheimnis zugegriffen wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis über den angegebenen Zeitraum hinaus nicht verwendet wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Zugriffszeitraum angeben, verwendet Security Hub CSPM einen Standardwert von 90 Tagen.

Das Löschen ungenutzter Geheimnisse ist genauso wichtig wie das Rotieren von Geheimnissen. Ungenutzte Geheimnisse können von ihren früheren Benutzern missbraucht werden, die keinen Zugriff mehr auf diese Geheimnisse benötigen. Da immer mehr Benutzer Zugriff auf ein Geheimnis erhalten, könnte es außerdem sein, dass jemand es falsch behandelt und an eine nicht autorisierte Stelle weitergegeben hat, was das Missbrauchsrisiko erhöht. Das Löschen ungenutzter Geheimnisse hilft dabei, Benutzern, die ihn nicht mehr benötigen, den geheimen Zugriff zu entziehen. Es hilft auch, die Kosten für die Verwendung von Secrets Manager zu senken. Daher ist es wichtig, ungenutzte Geheimnisse routinemäßig zu löschen.

Abhilfe

Informationen zum Löschen inaktiver Secrets Manager-Geheimnisse finden Sie unter Löschen eines AWS Secrets Manager Geheimnisses im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.6.3, PCI DSS v4.0. 1/8.3.9, CRI-Profil v2. 2/PR. AA-01.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-secret-periodic-rotation`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`maxDaysSinceRotation`	Maximale Anzahl von Tagen, an denen ein Geheimnis unverändert bleiben kann	Ganzzahl	1 auf `180`	`90`

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Geheimnis innerhalb des angegebenen Zeitrahmens mindestens einmal rotiert wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis nicht mindestens so häufig gewechselt wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Rotationszeitraum angeben, verwendet Security Hub CSPM einen Standardwert von 90 Tagen.

Das Rotieren von Geheimnissen kann Ihnen helfen, das Risiko einer unbefugten Verwendung Ihrer Geheimnisse in Ihrem zu verringern. AWS-Konto Beispiele hierfür sind Datenbankanmeldedaten, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebiger Text. Wenn Sie Ihre Geheimnisse über einen längeren Zeitraum nicht ändern, ist es wahrscheinlicher, dass die Geheimnisse kompromittiert werden.

Je mehr Benutzer Zugriff auf ein Geheimnis erhalten, desto wahrscheinlicher kann es sein, dass jemand falsch damit umgegangen ist und es an eine nicht autorisierte Person weitergegeben hat. Secrets können über Protokolle und Cache-Daten durchsickern. Sie werden ggf. für Debug-Zwecke freigegeben und nicht geändert oder widerrufen, wenn das Debugging abgeschlossen ist. Aus all diesen Gründen sollten Secrets regelmäßig rotiert werden.

Sie können die automatische Rotation von Geheimnissen in konfigurieren. AWS Secrets Manager Mit der automatischen Rotation können Sie langfristige Geheimnisse durch kurzfristige ersetzen,

wodurch das Risiko von Kompromissen erheblich reduziert wird. Wir empfehlen Ihnen, die automatische Rotation für Ihre Secrets Manager zu konfigurieren. Weitere Informationen finden Sie unter Rotieren von AWS Secrets Manager -Secrets im AWS Secrets Manager -Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config Regel: `tagged-secretsmanager-secret` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Secret Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement

schlägt fehl, wenn das Geheimnis keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Geheimnis mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Secrets Manager Manager-Geheimnis finden Sie unter AWS Secrets Manager Taggeheimnisse im AWS Secrets Manager Benutzerhandbuch.

Security Hub CSPM-Steuerungen für AWS Service Catalog

Dieses AWS Security Hub CSPM Steuerelement bewertet den AWS Service Catalog Dienst und die Ressourcen. Das Steuerelement ist möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8 NIST.800-53.r5 SC-7, CRI Profile v2. 2/PR. AA-04.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ServiceCatalog::Portfolio`

AWS Config -Regel: service-catalog-shared-within-organization

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS Service Catalog Portfolios innerhalb einer Organisation gemeinsam genutzt werden, wenn die Integration mit aktiviert AWS Organizations ist. Die Kontrolle schlägt fehl, wenn Portfolios nicht innerhalb einer Organisation gemeinsam genutzt werden.

Die Portfoliofreigabe nur innerhalb von Organizations trägt dazu bei, dass ein Portfolio nicht mit falschen Personen geteilt wird AWS-Konten. Um ein Servicekatalog-Portfolio mit einem Konto in einer Organisation zu teilen, empfiehlt Security Hub CSPM die Verwendung von `ORGANIZATION_MEMBER_ACCOUNT` anstelle von. `ACCOUNT` Dies vereinfacht die Verwaltung, da der Zugriff, der dem Konto gewährt wird, unternehmensweit geregelt wird. Wenn Sie aus geschäftlichen Gründen Service Catalog-Portfolios mit einem externen Konto teilen müssen, können Sie die Ergebnisse dieser Steuerung automatisch unterdrücken oder deaktivieren.

Abhilfe

Informationen zum Aktivieren der Portfolio-Sharing mit AWS Organizations finden Sie unter Teilen mit AWS Organizations im AWS Service Catalog Administratorhandbuch.

Security Hub CSPM-Steuerungen für Amazon SES

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen von Amazon Simple Email Service (Amazon SES).

Diese Kontrollen sind möglicherweise nicht in allen verfügbarAWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SES.1] SES-Kontaktlisten sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ContactList`

AWS ConfigRegel: `tagged-ses-contactlist` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon SES SES-Kontaktliste Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Kontaktliste keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Kontaktliste mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon SES-Kontaktliste finden Sie TagResourcein der Amazon SES API v2-Referenz.

[SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ConfigurationSet`

AWS ConfigRegel: `tagged-ses-configurationset` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWSAnforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon SES SES-Konfigurationssatz Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Konfigurationssatz keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Konfigurationssatz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglichAWS-Services, darunterAWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon SES-Konfigurationssatz finden Sie TagResourcein der Amazon SES API v2-Referenz.

[SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::SES::ConfigurationSet`

AWS Config-Regel: ses-sending-tls-required

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon SES SES-Konfigurationssatz TLS-Verbindungen erfordert. Die Steuerung schlägt fehl, wenn die TLS-Richtlinie `'REQUIRE'` für einen Konfigurationssatz nicht auf eingestellt ist.

Standardmäßig verwendet Amazon SES opportunistisches TLS, was bedeutet, dass E-Mails unverschlüsselt gesendet werden können, wenn keine TLS-Verbindung mit dem empfangenden E-Mail-Server hergestellt werden kann. Durch die Durchsetzung von TLS für den E-Mail-Versand wird sichergestellt, dass Nachrichten nur zugestellt werden, wenn eine sichere, verschlüsselte Verbindung hergestellt werden kann. Dies trägt zum Schutz der Vertraulichkeit und Integrität von E-Mail-Inhalten bei der Übertragung zwischen Amazon SES und dem E-Mail-Server des Empfängers bei. Wenn keine sichere TLS-Verbindung hergestellt werden kann, wird die Nachricht nicht zugestellt, wodurch die potenzielle Offenlegung vertraulicher Informationen verhindert wird.

> **Note**
>
> Obwohl TLS 1.3 die Standardzustellungsmethode für Amazon SES ist, ohne dass die TLS-Anforderungen durch Konfigurationssätze durchgesetzt werden, könnten Nachrichten möglicherweise im Klartext zugestellt werden, wenn eine TLS-Verbindung fehlschlägt. Um diese Kontrolle zu übergeben, müssen Sie die TLS-Richtlinie `'REQUIRE'` in den Zustellungsoptionen Ihres SES-Konfigurationssatzes entsprechend konfigurieren. Wenn TLS erforderlich ist, werden Nachrichten nur zugestellt, wenn eine TLS-Verbindung mit dem empfangenden Mailserver hergestellt werden kann.

Abhilfe

Informationen zur Konfiguration von Amazon SES so, dass TLS-Verbindungen für einen Konfigurationssatz erforderlich sind, finden Sie unter Amazon SES und Sicherheitsprotokolle im Amazon SES Developer Guide.

Security Hub CSPM-Steuerungen für Amazon SNS

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Notification Service (Amazon SNS). Die Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SNS.1] SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.11, 3.13.16, CRI Profile NIST.800-171.r2 v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::SNS::Topic`

AWS Config -Regel: `sns-encrypted-kms`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema im Ruhezustand mithilfe von Schlüsseln verschlüsselt ist, die in AWS Key Management Service (AWS KMS) verwaltet werden. Die Steuerung schlägt fehl, wenn das SNS-Thema keinen KMS-Schlüssel für die serverseitige Verschlüsselung (SSE) verwendet. Standardmäßig speichert SNS Nachrichten und Dateien mithilfe der Festplattenverschlüsselung. Um diese Kontrolle zu bestehen, müssen Sie stattdessen einen KMS-Schlüssel für die Verschlüsselung verwenden. Dies fügt eine zusätzliche Sicherheitsebene hinzu und bietet mehr Flexibilität bei der Zugriffskontrolle.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS API-Berechtigungen sind erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können. Wir empfehlen, SNS-Themen mit KMS-Schlüsseln zu verschlüsseln, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Aktivierung von SSE für ein SNS-Thema finden Sie unter Serverseitige Verschlüsselung (SSE) für ein Amazon SNS SNS-Thema aktivieren im Amazon Simple Notification Service Developer Guide. Bevor Sie SSE verwenden können, müssen Sie außerdem AWS KMS key Richtlinien konfigurieren, die die Verschlüsselung von Themen sowie die Verschlüsselung und Entschlüsselung von Nachrichten ermöglichen. Weitere Informationen finden Sie unter Konfiguration von AWS KMS Berechtigungen im Amazon Simple Notification Service Developer Guide.

[SNS.3] SNS-Themen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SNS::Topic`

AWS Config Regel: `tagged-sns-topic` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Thema keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Thema mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem SNS-Thema finden Sie unter Konfiguration von Amazon SNS SNS-Themen-Tags im Amazon Simple Notification Service Developer Guide.

[SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen

Verwandte Anforderungen: CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::SNS::Topic`

AWS Config -Regel: sns-topic-no-public-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Amazon SNS SNS-Themenzugriffsrichtlinie öffentlichen Zugriff zulässt. Diese Kontrolle schlägt fehl, wenn die SNS-Themenzugriffsrichtlinie den öffentlichen Zugriff zulässt.

Sie verwenden eine Amazon SNS SNS-Zugriffsrichtlinie mit einem bestimmten Thema, um einzuschränken, wer mit diesem Thema arbeiten kann (z. B. wer Nachrichten zu diesem Thema veröffentlichen oder wer es abonnieren kann). SNS-Richtlinien können anderen AWS-Konten oder Benutzern innerhalb Ihres eigenen Bereichs Zugriff gewähren. AWS-Konto Die Angabe eines Platzhalters (*) im `Principal` Feld der Themenrichtlinie und das Fehlen von Bedingungen zur Einschränkung der Themenrichtlinie können zu Datenexfiltration, Denial-of-Service oder unerwünschter Einschleusung von Nachrichten in Ihren Dienst durch einen Angreifer führen.

> **Note**
>
> Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Amazon SNS SNS-Zugriffsrichtlinie für ein Thema nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Aktualisierung der Zugriffsrichtlinien für ein SNS-Thema finden Sie unter Überblick über die Zugriffsverwaltung in Amazon SNS im Amazon Simple Notification Service Developer Guide.

Security Hub CSPM-Steuerelemente für Amazon SQS

Diese AWS Security Hub CSPM Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Queue Service (Amazon SQS). Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::SQS::Queue`

AWS Config Regel: `sqs-queue-encrypted` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Warteschlange nicht mit einem SQS-managed

Schlüssel (SSE-SQS) oder einem AWS Key Management Service (AWS KMS) Schlüssel (SSE-KMS) verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht autorisierter Benutzer auf Daten zugreift, die auf der Festplatte gespeichert sind. Server-side Verschlüsselung (SSE) schützt den Inhalt von Nachrichten in SQS-Warteschlangen mithilfe von SQS-managed Verschlüsselungsschlüsseln (SSE-SQS) oder AWS KMS Schlüsseln (). SSE-KMS

Abhilfe

Informationen zur Konfiguration von SSE für eine SQS-Warteschlange finden Sie unter Konfiguration der serverseitigen Verschlüsselung (SSE) für eine Warteschlange (Konsole) im Amazon Simple Queue Service Developer Guide.

[SQS.2] SQS-Warteschlangen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SQS::Queue`

AWS Config Regel: `tagged-sqs-queue` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Warteschlange keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Warteschlange mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer vorhandenen Warteschlange mithilfe der Amazon SQS SQS-Konsole finden Sie unter Konfiguration von Kostenzuweisungs-Tags für eine Amazon SQS SQS-Warteschlange (Konsole) im Amazon Simple Queue Service Developer Guide.

[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

Verwandte Anforderungen: CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. IR-01.01, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::SQS::Queue`

AWS Config -Regel: sqs-queue-no-public-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon SQS SQS-Zugriffsrichtlinie öffentlichen Zugriff auf eine SQS-Warteschlange ermöglicht. Die Kontrolle schlägt fehl, wenn eine SQS-Zugriffsrichtlinie öffentlichen Zugriff auf die Warteschlange ermöglicht.

Eine Amazon SQS SQS-Zugriffsrichtlinie kann den öffentlichen Zugriff auf eine SQS-Warteschlange ermöglichen, was einem anonymen Benutzer oder einer authentifizierten AWS IAM-Identität den Zugriff auf die Warteschlange ermöglichen kann. SQS-Zugriffsrichtlinien ermöglichen diesen Zugriff in der Regel durch Angabe des Platzhalterzeichens (`*`) im `Principal` Element der Richtlinie, ohne dass die richtigen Bedingungen verwendet werden, um den Zugriff auf die Warteschlange einzuschränken, oder beides. Wenn eine SQS-Zugriffsrichtlinie öffentlichen Zugriff zulässt, können Dritte möglicherweise Aufgaben wie das Empfangen von Nachrichten aus der Warteschlange, das Senden von Nachrichten an die Warteschlange oder das Ändern der Zugriffsrichtlinie für die Warteschlange ausführen. Dies kann zu Ereignissen wie Datenexfiltration, einem Denial-of-Service oder der Einschleusung von Nachrichten in die Warteschlange durch einen Bedrohungsakteur führen.

> **Note**
>
> Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein `PASSED` Ergebnis zu erzielen, dürfen Bedingungen in der Amazon SQS SQS-Zugriffsrichtlinie für eine Warteschlange nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen

zu Richtlinienvariablen finden Sie unter Variablen und Tags im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der SQS-Zugriffsrichtlinie für eine SQS-Warteschlange finden Sie unter Using custom policies with the Amazon SQS Access Policy Language im Amazon Simple Queue Service Developer Guide.

Security Hub CSPM-Steuerelemente für Step Functions

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Step Functions Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

Verwandte Anforderungen: PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::StepFunctions::StateMachine`

AWS Config -Regel: `step-functions-state-machine-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`logLevel`	Minimale Protokollierungsebene	Enum	`ALL`, `ERROR`, `FATAL`	Kein Standardwert

Mit dieser Steuerung wird geprüft, ob bei einer AWS Step Functions Zustandsmaschine die Protokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn auf einer Zustandsmaschine die Protokollierung nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `logLevel` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn für die Zustandsmaschine die angegebene Protokollierungsebene aktiviert ist.

Die Überwachung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Step Functions aufrechtzuerhalten. Sie sollten so viele Überwachungsdaten sammeln AWS-Services , wie Sie verwenden, damit Sie Fehler an mehreren Punkten leichter debuggen können. Wenn Sie eine Protokollierungskonfiguration für Ihre Step Functions Functions-Zustandsmaschinen definiert haben, können Sie den Ausführungsverlauf und die Ergebnisse in Amazon CloudWatch Logs verfolgen. Optional können Sie nur Fehler oder schwerwiegende Ereignisse verfolgen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Step Functions Functions-Zustandsmaschine finden Sie unter Protokollierung konfigurieren im AWS Step Functions Entwicklerhandbuch.

[StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::StepFunctions::Activity`

AWS Config Regel: `tagged-stepfunctions-activity` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Step Functions Aktivität Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Aktivität keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Aktivität mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Step Functions-Aktivität finden Sie unter Tagging in Step Functions im AWS Step Functions Entwicklerhandbuch.

Security Hub CSPM-Steuerelemente für Systems Manager

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Systems Manager (SSM) -Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

Verwandte Anforderungen: PCI DSS v3.2. 1/2.4, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8 (1) NIST.800-53.r5 CM-8, (2), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-15 NIST.800-53.r5 SI-2 (3) NIST.800-53.r5 SA-3, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Evaluierte Ressource: `AWS::EC2::Instance`

Erforderliche AWS Config Aufzeichnungsressourcen:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

AWS Config -Regel: ec2-instance-managed-by-systems-manager

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die gestoppten und laufenden EC2-Instances in Ihrem Konto von AWS Systems Manager verwaltet werden. Systems Manager ist ein AWS-Service Programm, mit dem Sie Ihre AWS Infrastruktur anzeigen und steuern können.

Um Sie bei der Aufrechterhaltung von Sicherheit und Compliance zu unterstützen, scannt Systems Manager Ihre gestoppten und laufenden verwalteten Instances. Eine verwaltete Instanz ist eine Maschine, die für die Verwendung mit Systems Manager konfiguriert ist. Systems Manager meldet dann alle festgestellten Richtlinienverstöße oder ergreift Korrekturmaßnahmen. Systems Manager hilft Ihnen auch, Ihre verwalteten Instances zu konfigurieren und zu verwalten. Weitere Informationen finden Sie im AWS Systems Manager -Benutzerhandbuch.

> **Note**
>
> Dieses Steuerelement generiert `FAILED` Ergebnisse für EC2-Instances, bei denen es sich um AWS Elastic Disaster Recovery Replication Server-Instances handelt, von denen sie verwaltet werden. AWS Eine Replication Server-Instance ist eine EC2-Instance, die automatisch von gestartet wird, AWS Elastic Disaster Recovery um die kontinuierliche Datenreplikation von Quellservern aus zu unterstützen. AWS entfernt absichtlich den Systems Manager (SSM) -Agenten aus diesen Instanzen, um die Isolation aufrechtzuerhalten und potenzielle unbeabsichtigte Zugriffspfade zu verhindern.

Abhilfe

Informationen zur Verwaltung von EC2-Instances mit AWS Systems Manager finden Sie unter Amazon EC2 EC2-Hostmanagement im AWS Systems Manager Benutzerhandbuch.
Im Bereich Konfigurationsoptionen auf der AWS Systems Manager Konsole können Sie die Standardeinstellungen beibehalten oder sie nach Bedarf für Ihre bevorzugte Konfiguration ändern.

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (3), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), NIST.800-171.r2 3.7.1, PCI DSS v3.2. 1/62.2, PCI DSS v4.0. 1/22.2.1, PCI-DSS v4.0. 1/6.3.3, CRI-Profil v2. 2/ID. RA-01.03, CRI-Profil v2. 2/PR. PS-02.01

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::SSM::PatchCompliance`

AWS Config -Regel: ec2-managedinstance-patch-compliance-status-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft, ob der Konformitätsstatus von Systems Manager Patch Compliance `COMPLIANT` oder `NON_COMPLIANT` nach der Patch-Installation auf der Instanz ist. Die Kontrolle schlägt fehl, wenn der Konformitätsstatus lautet`NON_COMPLIANT`. Das Steuerelement überprüft nur Instanzen, die von Systems Manager Patch Manager verwaltet werden.

Durch das Patchen Ihrer EC2-Instances gemäß den Anforderungen Ihres Unternehmens wird die Angriffsfläche Ihrer Instances reduziert. AWS-Konten

Abhilfe

Systems Manager empfiehlt die Verwendung von Patch-Richtlinien, um das Patchen für Ihre verwalteten Instanzen zu konfigurieren. Sie können auch Systems Manager Manager-Dokumente verwenden, wie im folgenden Verfahren beschrieben, um eine Instanz zu patchen.

So korrigieren Sie nicht konforme Patches

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie für Node Management die Option Befehl ausführen und anschließend Befehl ausführen aus.
3. Wählen Sie die Option für AWS- RunPatchBaseline.
4. Ändern Sie die Operation in Install (Installieren).
5. Wählen Sie Instanzen manuell auswählen und wählen Sie dann die nicht konformen Instanzen aus.
6. Klicken Sie auf Ausführen.
7. Wenn der Befehl abgeschlossen ist, wählen Sie im Navigationsbereich Compliance aus, um den neuen Compliance-Status Ihrer gepatchten Instances zu überwachen.

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8 (1) NIST.800-53.r5 CM-8, (3), NIST.800-53.r5 CM-8 NIST.800-53.r5 SI-2 (3), PCI DSS v3.2. 1/23.4, PCI DSS v4.0. 1/2.2.1, PCI DSS v4.0. 1/6.3.3, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/DE. CM-09.03, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-02.01, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. IR-01.03, CRI-Profil v2. 2/PR. IR-01.05

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::SSM::AssociationCompliance`

AWS Config -Regel: ec2-managedinstance-association-compliance-status-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Mit diesem Steuerelement wird geprüft, ob der Status der AWS Systems Manager Zuordnung auf einer Instanz den Status „Konformität“ hat `COMPLIANT` oder `NON_COMPLIANT` nachdem die Zuordnung ausgeführt wurde. Die Kontrolle schlägt fehl, wenn der Konformitätsstatus der Assoziation lautet`NON_COMPLIANT`.

Eine State Manager-Zuordnung ist eine Konfiguration, die Ihren verwalteten Instances zugewiesen ist. Die Konfiguration definiert den Status, den Sie auf Ihren Instances beibehalten möchten. Eine Zuordnung kann beispielsweise angeben, dass Antivirensoftware auf Ihren Instanzen installiert und ausgeführt werden muss oder dass bestimmte Ports geschlossen sein müssen.

Nachdem Sie eine oder mehrere State Manager-Zuordnungen erstellt haben, stehen Ihnen die Informationen zum Compliance-Status sofort zur Verfügung. Sie können den Konformitätsstatus in der Konsole oder als Reaktion auf AWS CLI Befehle oder entsprechende Systems Manager API-Aktionen anzeigen. Bei Zuordnungen zeigt Configuration Compliance den Konformitätsstatus (`Compliant`oder`Non-compliant`) an. Außerdem wird der Schweregrad angezeigt, der der Zuordnung zugewiesen wurde, z. B. `Critical` oder`Medium`.

Weitere Informationen zur Einhaltung der State Manager-Zuordnungen finden Sie im AWS Systems Manager Benutzerhandbuch unter Informationen zur Einhaltung von State Manager-Zuordnungen.

Abhilfe

Eine fehlgeschlagene Zuordnung kann auf verschiedene Dinge zurückzuführen sein, z. B. auf Ziele und Systems Manager Manager-Dokumentnamen. Um dieses Problem zu beheben, müssen Sie zunächst die Zuordnung identifizieren und untersuchen, indem Sie sich den Zuordnungsverlauf ansehen. Anweisungen zum Anzeigen des Zuordnungsverlaufs finden Sie unter Zuordnungshistorien anzeigen im AWS Systems Manager Benutzerhandbuch.

Nach der Untersuchung können Sie die Zuordnung bearbeiten, um das festgestellte Problem zu beheben. Sie können eine Zuordnung bearbeiten, um den Namen, den Zeitplan, den Schweregrad oder die Ziele zu ändern. Nachdem Sie eine Zuordnung bearbeitet haben, AWS Systems Manager wird eine neue Version erstellt. Anweisungen zum Bearbeiten einer Zuordnung finden Sie im AWS Systems Manager Benutzerhandbuch unter Bearbeiten und Erstellen einer neuen Version einer Zuordnung.

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. IR-01.01

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::SSM::Document`

AWS Config -Regel: ssm-document-not-public

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Kontrolle wird geprüft, ob AWS Systems Manager Dokumente, die einem Konto gehören, öffentlich sind. Die Kontrolle schlägt fehl, wenn Systems Manager Manager-Dokumente, die den Eigentümer haben`Self`, öffentlich sind.

Öffentliche Systems Manager Manager-Dokumente ermöglichen möglicherweise unbeabsichtigten Zugriff auf Ihre Dokumente. Ein öffentliches Systems Manager Manager-Dokument kann wertvolle Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse enthalten.

Sofern Ihr Anwendungsfall die öffentliche Freigabe nicht erfordert, empfehlen wir, die öffentliche Freigabe für Systems Manager Manager-Dokumente zu blockieren, die den Eigentümer haben`Self`.

Abhilfe

Informationen zur Konfiguration der gemeinsamen Nutzung von Systems Manager Manager-Dokumenten finden Sie unter Freigeben eines SSM-Dokuments im AWS Systems Manager Benutzerhandbuch.

[SSM.5] SSM-Dokumente sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SSM::Document`

AWS Config -Regel: ssm-document-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Systems Manager Dokument über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Das Steuerelement schlägt fehl, wenn das Dokument keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Dokument keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben. Die Kontrolle bewertet keine Systems Manager Manager-Dokumente, die Amazon gehören.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einem AWS Systems Manager Dokument Tags hinzuzufügen, können Sie den AddTagsToResourceBetrieb der AWS Systems Manager API verwenden oder, falls Sie den verwenden AWS CLI, den Befehl add-tags-to-resource ausführen. Sie können auch die AWS Systems Manager -Konsole verwenden.

[SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch

Verwandte Anforderungen: CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: ssm-automation-logging-enabled

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob die CloudWatch Amazon-Protokollierung für AWS Systems Manager (SSM) Automation aktiviert ist. Die Kontrolle schlägt fehl, wenn die CloudWatch Protokollierung für SSM Automation nicht aktiviert ist.

SSM Automation ist ein AWS Systems Manager Tool, mit dem Sie automatisierte Lösungen für die skalierbare Bereitstellung, Konfiguration und Verwaltung von AWS Ressourcen mithilfe vordefinierter oder benutzerdefinierter Runbooks erstellen können. Um die Betriebs- oder Sicherheitsanforderungen für Ihr Unternehmen zu erfüllen, müssen Sie möglicherweise eine Aufzeichnung der ausgeführten Skripts bereitstellen. Sie können SSM Automation so konfigurieren, dass die Ausgabe von `aws:executeScript` Aktionen in Ihren Runbooks an eine von Ihnen angegebene Amazon CloudWatch Logs-Protokollgruppe gesendet wird. Mit CloudWatch Logs können Sie Protokolldateien aus verschiedenen Quellen überwachen, speichern und darauf zugreifen. AWS-Services

Abhilfe

Informationen zur Aktivierung der CloudWatch Protokollierung für SSM Automation finden Sie unter Ausgabe der Automatisierungsaktion protokollieren mit CloudWatch Protokollen im AWS Systems Manager Benutzerhandbuch.

[SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein

Verwandte Anforderungen: CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. AA-01.02, CRI-Profil v2. 2/PR. AA-03.02, CRI-Profil v2. 2/PR. AA-05.01, CRI-Profil v2. 2/PR. PS-01.01, CRI-Profil v2. 2/PR. PS-01.02

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: ssm-automation-block-public-sharing

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Einstellung Öffentliche Freigabe blockieren für AWS Systems Manager Dokumente aktiviert ist. Die Steuerung schlägt fehl, wenn die Einstellung Öffentliche Freigabe blockieren für Systems Manager Manager-Dokumente deaktiviert ist.

Die Einstellung „Öffentliches Teilen von Dokumenten blockieren“ AWS Systems Manager (SSM) ist eine Einstellung auf Kontoebene. Durch die Aktivierung dieser Einstellung kann unerwünschter Zugriff auf Ihre SSM-Dokumente verhindert werden. Wenn Sie diese Einstellung aktivieren, wirkt sich Ihre Änderung nicht auf SSM-Dokumente aus, die Sie derzeit für die Öffentlichkeit freigeben. Sofern Ihr Anwendungsfall nicht erfordert, dass Sie SSM-Dokumente für die Öffentlichkeit freigeben, empfehlen wir Ihnen, die Einstellung „Öffentliches Teilen blockieren“ zu aktivieren. Die Einstellung kann für jede AWS-Region Einstellung unterschiedlich sein.

Abhilfe

Informationen zur Aktivierung der Einstellung „Öffentliches Teilen blockieren“ für Dokumente AWS Systems Manager (SSM) finden Sie im AWS Systems Manager Benutzerhandbuch unter Öffentliche Freigabe für SSM-Dokumente blockieren.

Security Hub CSPM-Steuerungen für AWS Transfer Family

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS Transfer Family Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Transfer.1] AWS Transfer Family Workflows sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Workflow`

AWS Config Regel: `tagged-transfer-workflow` (benutzerdefinierte Security Hub CSPM-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	`No default value`

Dieses Steuerelement prüft, ob ein AWS Transfer Family Workflow Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Workflow keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Workflow mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Stichwörter zu einem Transfer Family Family-Workflow hinzu (Konsole)

1. Öffnen Sie die AWS Transfer Family Konsole.
2. Wählen Sie im Navigationsbereich die Option Workflows aus. Wählen Sie dann den Workflow aus, den Sie taggen möchten.
3. Wählen Sie Tags verwalten aus und fügen Sie dann die Tags hinzu.

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

Verwandte Anforderungen: NIST.800-53.r5 CM-7,, NIST.800-53.r5 IA-5 NIST.800-53.r5 SC-8, PCI DSS v4.0. 1/4.2.1, CRI-Profil v2. 2/PR. DS-02.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Transfer::Server`

AWS Config -Regel: transfer-family-server-no-ftp

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Transfer Family Server ein anderes Protokoll als FTP für die Endpunktverbindung verwendet. Die Steuerung schlägt fehl, wenn der Server das FTP-Protokoll verwendet, damit ein Client eine Verbindung zum Serverendpunkt herstellt.

FTP (File Transfer Protocol) stellt die Endpunktverbindung über unverschlüsselte Kanäle her, sodass Daten, die über diese Kanäle gesendet werden, abgefangen werden können. Die Verwendung von

SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) oder AS2 (Applicability Statement 2) bietet eine zusätzliche Sicherheitsebene, indem Ihre Daten während der Übertragung verschlüsselt werden, und kann dazu beitragen, potenzielle Angreifer daran zu hindern, Person-in-the-Middle- oder ähnliche Angriffe durchzuführen, um den Netzwerkverkehr zu belauschen oder zu manipulieren.

Abhilfe

Informationen zum Ändern des Protokolls für einen Transfer Family Family-Server finden Sie unter Bearbeiten der Dateiübertragungsprotokolle im AWS Transfer Family Benutzerhandbuch.

[Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (7), NIST.800-53.r5 AU-9 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8),, NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/DE. AE-03.02, CRI-Profil v2. 2/DE. CM-03.01, CRI-Profil v2. 2/DE. CM-03.02, CRI-Profil v2. 2/DE. CM-03.03, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Transfer::Connector`

AWS Config -Regel: transfer-connector-logging-enabled

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die CloudWatch Amazon-Protokollierung für einen AWS Transfer Family Connector aktiviert ist. Die Steuerung schlägt fehl, wenn die CloudWatch Protokollierung für den Connector nicht aktiviert ist.

Amazon CloudWatch ist ein Überwachungs- und Beobachtbarkeitsservice, der Einblick in Ihre AWS Ressourcen, einschließlich AWS Transfer Family Ressourcen, bietet. For Transfer Family

CloudWatch bietet eine konsolidierte Prüfung und Protokollierung des Workflow-Fortschritts und der Ergebnisse. Dazu gehören mehrere Metriken, die Transfer Family für Workflows definiert. Sie können Transfer Family so konfigurieren, dass Connector-Ereignisse automatisch protokolliert CloudWatch werden. Dazu geben Sie eine Protokollierungsrolle für den Connector an. Für die Protokollierungsrolle erstellen Sie eine IAM-Rolle und eine ressourcenbasierte IAM-Richtlinie, die die Berechtigungen für die Rolle definiert.

Abhilfe

Informationen zur Aktivierung der CloudWatch Protokollierung für einen Transfer Family Family-Connector finden Sie unter CloudWatch Amazon-Protokollierung für AWS Transfer Family Server im AWS Transfer Family Benutzerhandbuch.

[Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Agreement`

AWS Config -Regel: transfer-agreement-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
	Groß- und Kleinschreibung unterschieden.			

Dieses Steuerelement prüft, ob eine AWS Transfer Family Vereinbarung die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Das Steuerelement schlägt fehl, wenn die Vereinbarung keine Tagschlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Vereinbarung keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS Transfer Family Vereinbarung finden Sie unter Methoden zur Kennzeichnung von Ressourcen für AWS Ressourcen und Tag-Editor.

[Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Certificate`

AWS Config -Regel: transfer-certificate-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Zertifikat über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Die Steuerung schlägt fehl, wenn das Zertifikat keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu

kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Transfer Family Zertifikat finden Sie unter Methoden zur Kennzeichnung von Ressourcen für Ressourcen und Tag-Editor im Benutzerhandbuch zur Kennzeichnung von AWS Ressourcen und Tag-Editor.

[Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein

Verwandte Anforderungen: CRI-Profil v2. 2/ID. AM-02.01, CRI-Profil v2. 2/ID. AM-05.01

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Connector`

AWS Config -Regel: transfer-connector-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Konnektor über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Konnektor keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Konnektor keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Transfer Family Connector finden Sie unter Methoden zur Kennzeichnung von Ressourcen für AWS Ressourcen und Tag-Editor für Ressourcen mit Tags.

[Transfer.7] Familienprofile übertragen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Profile`

AWS Config -Regel: transfer-profile-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Description	Typ	Zulässige benutzerdefinierte Werte	Security Hub CSPM-Standardwert
`requiredKeyTags`	Eine Liste von Schlüsseln für das Tag 'n', die einer evaluierten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Profil die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Das Steuerelement schlägt fehl, wenn das Profil keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Profil keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben. Das Steuerelement wertet lokale Profile und Partnerprofile aus.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im Tagging AWS Resources and Tag Editor User Guide.

> **Note**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einem AWS Transfer Family Profil finden Sie unter Methoden zur Kennzeichnung von Ressourcen für AWS Ressourcen und Tag-Editor.

Security Hub CSPM-Steuerungen für AWS WAF

Diese AWS Security Hub CSPM Kontrollen bewerten den AWS WAF Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::WebACL`

AWS Config -Regel: `waf-classic-logging-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS WAF globale Web-ACL aktiviert ist. Dieses Steuerelement schlägt fehl, wenn die Protokollierung für die Web-ACL nicht aktiviert ist.

Die Protokollierung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS WAF Global. Sie ist in vielen Unternehmen eine Geschäfts- und Compliance-Anforderung und ermöglicht es Ihnen, Fehler beim Verhalten von Anwendungen zu beheben. Es enthält auch detaillierte Informationen über den Datenverkehr, der von der angehängten Web-ACL analysiert wird AWS WAF.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine AWS WAF Web-ACL finden Sie unter Logging Web-ACL-Verkehrsinformationen im AWS WAF Developer Guide.

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::Rule`

AWS Config -Regel: `waf-regional-rule-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF Regionalregel mindestens eine Bedingung hat. Die Steuerung schlägt fehl, wenn in einer Regel keine Bedingungen erfüllt sind.

Eine regionale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Verkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Wenn keine Bedingungen erfüllt sind, wird der Verkehr ohne Inspektion weitergeleitet. Eine WAF-Regionalregel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen einer Bedingung zu einer leeren Regel finden Sie unter Hinzufügen und Entfernen von Bedingungen in einer Regel im AWS WAF Entwicklerhandbuch.

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::RuleGroup`

AWS Config -Regel: `waf-regional-rulegroup-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF regionale Regelgruppe mindestens eine Regel hat. Die Steuerung schlägt fehl, wenn in einer Regelgruppe keine Regeln vorhanden sind.

Eine regionale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Datenverkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine regionale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen von Regeln und Regelbedingungen zu einer leeren Regelgruppe finden Sie unter Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe und Hinzufügen und Entfernen von Bedingungen in einer Regel im AWS WAF Entwicklerhandbuch.

[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::WebACL`

AWS Config -Regel: `waf-regional-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF Classic Regional Web-ACL WAF-Regeln oder WAF-Regelgruppen enthält. Dieses Steuerelement schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder Regelgruppen enthält.

Eine regionale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-Traffic je nach Standardaktion weitergeleitet werden, ohne von der WAF erkannt oder bearbeitet zu werden.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF Classic Regional Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch.

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::Rule`

AWS Config -Regel: `waf-global-rule-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Regel Bedingungen enthält. Das Steuerelement schlägt fehl, wenn in einer Regel keine Bedingungen erfüllt sind.

Eine globale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen einer Regel ermöglichen die Überprüfung des Datenverkehrs und die Durchführung einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne jegliche Bedingungen wird der Verkehr ohne Inspektion weitergeleitet. Eine globale WAF-Regel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Erstellen einer Regel und zum Hinzufügen von Bedingungen finden Sie unter Regel erstellen und Bedingungen hinzufügen im AWS WAF Entwicklerhandbuch.

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.03

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::RuleGroup`

AWS Config -Regel: `waf-global-rulegroup-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Regelgruppe mindestens eine Regel hat. Das Steuerelement schlägt fehl, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Eine globale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Datenverkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine globale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Hinzufügen einer Regel zu einer Regelgruppe finden Sie unter Creating an AWS WAF Classic Rule Group im AWS WAF Developer Guide.

[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), CRI-Profil v2. 2/DE. CM-01.01, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::WebACL`

AWS Config -Regel: `waf-global-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Web-ACL mindestens eine WAF-Regel oder WAF-Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder Regelgruppen enthält.

Eine globale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-Traffic je nach Standardaktion weitergeleitet werden, ohne von der WAF erkannt oder bearbeitet zu werden.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF globalen Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch. Wählen Sie für Filter die Option Global (CloudFront).

[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI-Profil v2. 2/DE. CM-01.03, CRI-Profil v2. 2/PR. IR-01.02, CRI-Profil v2. 2/PR. PS-01.01

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFv2::WebACL`

AWS Config -Regel: `wafv2-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF V2-Web-Zugriffskontrollliste (Web-ACL) mindestens eine Regel oder Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine Regeln oder Regelgruppen enthält.

Eine Web-ACL gibt Ihnen eine detaillierte Kontrolle über alle HTTP (S) -Webanfragen, auf die Ihre geschützte Ressource reagiert. Eine Web-ACL sollte eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-

Traffic AWS WAF je nach Standardaktion weitergeleitet werden, ohne dass er erkannt oder bearbeitet wird.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren WAF2-Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch.

[WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12,, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (10) NIST.800-53.r5 CA-7, (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/PR. PS-04.01, CRI-Profil v2. 2/PR. PS-04.02, CRI-Profil v2. 2/PR. PS-04.03

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::WAFv2::WebACL`

AWS Config Regel: **`wafv2-logging-enabled`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS WAF V2-Webzugriffskontrollliste (Web-ACL) aktiviert ist. Diese Kontrolle schlägt fehl, wenn die Protokollierung für die Web-ACL deaktiviert ist.

> **Note**
>
> Dieses Steuerelement überprüft nicht, ob die AWS WAF Web-ACL-Protokollierung für ein Konto über Amazon Security Lake aktiviert ist.

Durch die Protokollierung wird die Zuverlässigkeit, Verfügbarkeit und Leistung von aufrechterhalten AWS WAF. Darüber hinaus ist die Protokollierung in vielen Organisationen eine Geschäfts- und Compliance-Anforderung. Durch die Protokollierung des Datenverkehrs, der von Ihrer Web-ACL analysiert wird, können Sie Fehler beim Verhalten von Anwendungen beheben.

Abhilfe

Informationen zur Aktivierung der Protokollierung für eine AWS WAF Web-ACL finden Sie unter Verwaltung der Protokollierung für eine Web-ACL im AWS WAF Entwicklerhandbuch.

[WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),, NIST.800-53.r5 SC-7 (10) NIST.800-53.r5 CA-7, (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, CRI-Profil v2. 2/DE. AE-02.01, CRI-Profil v2. 2/DE. AE-02.02, CRI-Profil v2. 2/DE. AE-03.01, CRI-Profil v2. 2/RS. MA-02.01

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::WAFv2::RuleGroup`

AWS Config Regel: **`wafv2-rulegroup-logging-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS WAF Regel oder Regelgruppe CloudWatch Amazon-Metriken aktiviert sind. Die Kontrolle schlägt fehl, wenn für die Regel oder Regelgruppe keine CloudWatch Metriken aktiviert sind.

Durch die Konfiguration von CloudWatch Metriken AWS WAF für Regeln und Regelgruppen erhalten Sie Einblick in den Verkehrsfluss. Sie können sehen, welche ACL-Regeln ausgelöst werden und welche Anfragen akzeptiert und blockiert werden. Diese Sichtbarkeit kann Ihnen helfen, böswillige Aktivitäten auf Ihren verknüpften Ressourcen zu erkennen.

Abhilfe

Rufen Sie die UpdateRuleGroupAPI auf, um CloudWatch Metriken für eine AWS WAF Regelgruppe zu aktivieren. Rufen Sie die UpdateWebACL-API auf, um CloudWatch Metriken für eine AWS WAF Regel zu aktivieren. Stellen Sie das `CloudWatchMetricsEnabled` Feld auf ein. `true` Wenn Sie die AWS WAF Konsole verwenden, um Regeln oder Regelgruppen zu erstellen, werden CloudWatch Metriken automatisch aktiviert.

Security Hub CSPM-Steuerungen für WorkSpaces

Diese AWS Security Hub CSPM Kontrollen bewerten den WorkSpaces Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: CRI Profile v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::WorkSpaces::Workspace`

AWS Config -Regel: `workspaces-user-volume-encryption-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Benutzervolume in einem Amazon im Ruhezustand verschlüsselt WorkSpaces WorkSpace ist. Die Kontrolle schlägt fehl, wenn das WorkSpace Benutzervolume im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Verschlüsseln eines WorkSpaces Benutzervolumes finden Sie unter Encrypt a WorkSpace im WorkSpaces Amazon-Administratorhandbuch.

[WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: CRI-Profil v2. 2/PR. DS-01.01, CRI-Profil v2. 2/PR. PS-01.06, CRI-Profil v2. 2/PR. PS-01.08

Kategorie: Schützen > Datenschutz > Verschlüsselung ruhender Daten

Schweregrad: Mittel

Art der Ressource: `AWS::WorkSpaces::Workspace`

AWS Config -Regel: `workspaces-root-volume-encryption-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Root-Volume in einem Amazon im Ruhezustand verschlüsselt WorkSpaces WorkSpace ist. Die Kontrolle schlägt fehl, wenn das WorkSpace Root-Volume im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Verschlüsseln eines WorkSpaces Root-Volumes finden Sie unter Encrypt a WorkSpace im WorkSpaces Amazon-Administratorhandbuch.

Erforderliche Berechtigungen zur Konfiguration von Steuerelementen in Security Hub CSPM

Um Informationen über Sicherheitskontrollen anzuzeigen und Sicherheitskontrollen in Standards zu aktivieren und zu deaktivieren, benötigt die AWS Identity and Access Management (IAM) -Rolle, die Sie für den Zugriff auf AWS Security Hub CSPM verwenden, Berechtigungen, um die folgenden Operationen der Security Hub CSPM-API aufzurufen.

Um die erforderlichen Berechtigungen zu erhalten, können Sie verwaltete Security Hub CSPM-Richtlinien verwenden. Alternativ können Sie benutzerdefinierte IAM-Richtlinien so aktualisieren, dass sie auch Berechtigungen für diese Aktionen enthalten.

- BatchGetSecurityControls— Gibt Informationen zu einer Reihe von Sicherheitskontrollen für das Girokonto zurück undAWS-Region.
- ListSecurityControlDefinitions— Gibt Informationen über Sicherheitskontrollen zurück, die für einen bestimmten Standard gelten.

- ListStandardsControlAssociations— Identifiziert, ob eine Sicherheitskontrolle derzeit in jedem aktivierten Standard im Konto aktiviert oder deaktiviert ist.
- BatchGetStandardsControlAssociations— Identifiziert für eine Reihe von Sicherheitskontrollen, ob die einzelnen Kontrollen derzeit in einem bestimmten Standard aktiviert oder deaktiviert sind.
- BatchUpdateStandardsControlAssociations— Wird verwendet, um eine Sicherheitskontrolle in Standards zu aktivieren, die die Steuerung enthalten, oder um eine Steuerung in Standards zu deaktivieren. Dies ist ein Batch-Ersatz für den bestehenden `UpdateStandardsControl`Vorgang.
- BatchUpdateStandardsControlAssociations— Wird verwendet, um eine Reihe von Sicherheitskontrollen in Standards zu aktivieren oder zu deaktivieren, die diese Kontrollen enthalten. Dies ist ein Batch-Ersatz für den bestehenden `UpdateStandardsControl`Vorgang.
- UpdateStandardsControl— Wird verwendet, um eine einzelne Sicherheitskontrolle in Standards zu aktivieren oder zu deaktivieren, die die Steuerung beinhalten
- DescribeStandardsControl— Gibt Details zu den angegebenen Sicherheitskontrollen zurück.

Zusätzlich zu den oben genannten APIs sollten Sie Ihrer IAM-Rolle die Berechtigung `BatchGetControlEvaluations` zum Aufrufen hinzufügen. Diese Berechtigung ist erforderlich, um den Aktivierungs- und Konformitätsstatus einer Kontrolle, die Ergebnisse für eine Kontrolle und die Gesamtsicherheitsbewertung für Kontrollen auf der Security Hub CSPM-Konsole einzusehen. Da nur die Konsole aufruft`BatchGetControlEvaluations`, entspricht diese Berechtigung nicht direkt den öffentlich dokumentierten Security Hub CSPM-APIs oder AWS CLI -Befehlen.

Steuerelemente in Security Hub CSPM aktivieren

In AWS Security Hub CSPM ist eine Kontrolle eine Schutzmaßnahme innerhalb eines Sicherheitsstandards, die einer Organisation hilft, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Informationen zu schützen. Jede Security Hub CSPM-Steuerung bezieht sich auf eine bestimmte Ressource. AWS Wenn Sie ein Steuerelement aktivieren, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsprüfungen für das Steuerelement und generiert entsprechende Ergebnisse. Security Hub CSPM berücksichtigt bei der Berechnung der Sicherheitswerte auch alle aktivierten Kontrollen.

Sie können wählen, ob Sie eine Kontrolle für alle Sicherheitsstandards aktivieren möchten, für die sie gilt. Alternativ können Sie den Aktivierungsstatus in verschiedenen Standards unterschiedlich konfigurieren. Wir empfehlen die erstgenannte Option, bei der der Aktivierungsstatus eines Steuerelements für alle aktivierten Standards einheitlich ist. Anweisungen dazu, wie Sie ein Steuerelement standardübergreifend aktivieren und es anwenden, finden Sie unter. Ein

standardübergreifendes Steuerelement aktivieren Anweisungen zum Aktivieren einer Steuerung in bestimmten Standards finden Sie unterAktivierung einer Steuerung in einem bestimmten Standard.

Wenn Sie die regionsübergreifende Aggregation aktivieren und sich bei einer Aggregationsregion anmelden, zeigt die Security Hub CSPM-Konsole Steuerelemente an, die in mindestens einer verknüpften Region verfügbar sind. Wenn ein Steuerelement in einer verknüpften Region, aber nicht in der Aggregationsregion verfügbar ist, können Sie dieses Steuerelement in der Aggregationsregion nicht aktivieren oder deaktivieren.

Sie können Steuerelemente in jeder Region mithilfe der Security Hub CSPM-Konsole, der Security Hub CSPM-API oder aktivieren und deaktivieren. AWS CLI

Die Anweisungen zum Aktivieren und Deaktivieren der Steuerelemente variieren je nachdem, ob Sie die zentrale Konfiguration verwenden oder nicht. ??? In diesem Thema werden die Unterschiede beschrieben. Die zentrale Konfiguration steht Benutzern zur Verfügung, die Security Hub CSPM und integrieren. AWS Organizations Wir empfehlen, die zentrale Konfiguration zu verwenden, um das Aktivieren und Deaktivieren von Steuerelementen in Umgebungen mit mehreren Konten und mehreren Regionen zu vereinfachen. Wenn Sie die zentrale Konfiguration verwenden, können Sie mithilfe von Konfigurationsrichtlinien eine Steuerung für mehrere Konten und Regionen aktivieren. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie in jeder Region und jedem Konto separat ein Steuerelement aktivieren.

Ein standardübergreifendes Steuerelement aktivieren

Wir empfehlen, ein AWS Security Hub CSPM-Steuerelement für alle Standards zu aktivieren, für die das Steuerelement gilt. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein Ergebnis pro Kontrollüberprüfung, auch wenn eine Kontrolle zu mehr als einem Standard gehört.

Cross-standard Aktivierung in Umgebungen mit mehreren Konten und mehreren Regionen

Um eine Sicherheitskontrolle über mehrere Kanäle hinweg zu aktivieren AWS-Regionen, müssen Sie mit dem delegierten Security Hub CSPM-Administratorkonto angemeldet sein AWS-Konten und die zentrale Konfiguration verwenden. ???

Bei der zentralen Konfiguration kann der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die bestimmte Kontrollen über aktivierte Standards hinweg ermöglichen. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten und Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können sich beispielsweise dafür entscheiden, alle Steuerelemente in einer Organisationseinheit zu aktivieren, und Sie können sich dafür entscheiden, nur Amazon Elastic Compute Cloud (EC2) -Steuerelemente in einer anderen Organisationseinheit zu aktivieren. Der Grad der Granularität hängt von Ihren beabsichtigten Sicherheitszielen in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte standardübergreifende Kontrollen ermöglicht, finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um die Kontrollen in allen Standards außer dem Service-Managed Standard: AWS Control Tower zu verwalten. Die Steuerungen für diesen Standard sollten im AWS Control Tower Dienst konfiguriert werden.

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerelemente konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet festlegen. Self-managed Konten müssen die Steuerelemente in jeder Region separat konfigurieren.

Cross-standard Aktivierung für ein einzelnes Konto und eine einzelne Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto sind, können Sie Konfigurationsrichtlinien nicht verwenden, um Steuerungen in mehreren Konten und Regionen zentral zu aktivieren. Sie können jedoch die folgenden Schritte ausführen, um eine Steuerung in einem einzelnen Konto und einer Region zu aktivieren.

Security Hub CSPM console

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich die Option Steuerelemente aus.
3. Wählen Sie die Registerkarte Deaktiviert.
4. Wählen Sie die Option neben einem Steuerelement.
5. Wählen Sie „Steuerung aktivieren“ (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist).

6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Security Hub CSPM API

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu aktivieren

1. Rufen Sie die ListStandardsControlAssociations API auf. Geben Sie eine Sicherheitskontroll-ID an.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Rufen Sie die BatchUpdateStandardsControlAssociations API auf. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen das Steuerelement nicht aktiviert ist. Um Standard-ARNs abzurufen, führen Sie `DescribeStandards` den Befehl aus.
3. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`ENABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
   best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
   }
   ```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement aktivieren möchten.

AWS CLI

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu aktivieren

1. Führen Sie den Befehl list-standards-control-associations aus. Geben Sie eine Sicherheitskontroll-ID ein.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen die Steuerung nicht aktiviert ist. Führen Sie den `describe-standards` Befehl aus, um Standard-ARNs abzurufen.
3. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`ENABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Aktivierung einer Steuerung in einem bestimmten Standard

Wenn Sie einen Standard in AWS Security Hub CSPM aktivieren, werden alle für ihn geltenden Steuerelemente automatisch in diesem Standard aktiviert (eine Ausnahme bilden dienstverwaltete Standards). Anschließend können Sie bestimmte Steuerelemente im Standard deaktivieren und erneut aktivieren. Wir empfehlen jedoch, den Aktivierungsstatus einer Steuerung auf alle aktivierten Standards abzustimmen. Anweisungen zum Aktivieren einer Steuerung für alle Standards finden Sie unter. Ein standardübergreifendes Steuerelement aktivieren

Die Detailseite für einen Standard enthält die Liste der anwendbaren Kontrollen für den Standard sowie Informationen darüber, welche Steuerelemente derzeit in diesem Standard aktiviert und deaktiviert sind.

Auf der Standarddetailseite können Sie auch Steuerelemente in bestimmten Standards aktivieren. Sie müssen die Steuerelemente in bestimmten Standards in jedem AWS-Konto und separat aktivieren AWS-Region. Wenn Sie ein Steuerelement in bestimmten Standards aktivieren, wirkt sich dies nur auf das Girokonto und die Region aus.

Um ein Steuerelement in einem Standard zu aktivieren, müssen Sie zuerst mindestens einen Standard aktivieren, für den das Steuerelement gilt. Anweisungen zum Aktivieren eines Standards finden Sie unterEinen Sicherheitsstandard aktivieren. Wenn Sie ein Steuerelement in einem oder mehreren Standards aktivieren, beginnt Security Hub CSPM, Ergebnisse für dieses Steuerelement zu generieren. Security Hub CSPM bezieht den Kontrollstatus in die Berechnung der Gesamtsicherheitsbewertung und der Standardsicherheitsbewertungen ein. Selbst wenn Sie eine Kontrolle in mehreren Standards aktivieren, erhalten Sie pro standardübergreifender Sicherheitsüberprüfung ein einziges Ergebnis, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Weitere Informationen finden Sie unter Konsolidierte Erkenntnisse zu Kontrollen.

Um eine Kontrolle in einem Standard zu aktivieren, muss die Kontrolle in Ihrer aktuellen Region verfügbar sein. Weitere Informationen finden Sie unter Verfügbarkeit von Steuerelementen nach Regionen.

Gehen Sie wie folgt vor, um eine Security Hub CSPM-Steuerung in einem bestimmten Standard zu aktivieren. Anstelle der folgenden Schritte können Sie auch die `UpdateStandardsControl` API-Aktion verwenden, um Steuerelemente in einem bestimmten Standard zu aktivieren. Anweisungen zum Aktivieren einer Steuerung in allen Standards finden Sie unterCross-standard Aktivierung für ein einzelnes Konto und eine einzelne Region.

Security Hub CSPM console

So aktivieren Sie ein Steuerelement in einem bestimmten Standard

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus.
3. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
4. Wählen Sie ein Steuerelement aus.
5. Wählen Sie „Steuerung aktivieren“ (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist). Bestätigen Sie, indem Sie „Aktivieren“ wählen.

Security Hub CSPM API

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie `ListSecurityControlDefinitions` den Befehl aus und geben Sie einen Standard-ARN ein, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Um einen Standard-ARN zu erhalten, führen Sie den Befehl aus `DescribeStandards`. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Führen Sie aus `ListStandardsControlAssociations` und geben Sie eine bestimmte Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Führen Sie `BatchUpdateStandardsControlAssociations`. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`ENABLED`.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
   }
   ```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie den `list-security-control-definitions` Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Um einen Standard-ARN zu erhalten, führen Sie den Befehl aus`describe-standards`. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den `list-standards-control-associations` Befehl aus und geben Sie eine bestimmte Kontroll-ID an, um den aktuellen Aktivierungsstatus einer Steuerung in jedem Standard zurückzugeben.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Führen Sie den Befehl `batch-update-standards-control-associations` aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Automatisches Aktivieren neuer Steuerungen in aktivierten Standards

AWSSecurity Hub CSPM veröffentlicht regelmäßig neue Kontrollen und fügt sie zu einem oder mehreren Standards hinzu. Sie können wählen, ob neue Kontrollen in Ihren aktivierten Standards automatisch aktiviert werden sollen.

Wir empfehlen, die zentrale Security Hub CSPM-Konfiguration zu verwenden, um neue Sicherheitskontrollen automatisch zu aktivieren. Sie können Konfigurationsrichtlinien erstellen, die

eine Liste von Kontrollen enthalten, die standardübergreifend deaktiviert werden sollen. Alle anderen Steuerelemente, einschließlich der neu veröffentlichten, sind standardmäßig aktiviert. Alternativ können Sie Richtlinien erstellen, die eine Liste von Kontrollen enthalten, die standardübergreifend aktiviert werden sollen. Alle anderen Kontrollen, einschließlich der neu veröffentlichten, sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter Grundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Security Hub CSPM aktiviert keine neuen Steuerelemente, wenn sie zu einem Standard hinzugefügt werden, den Sie nicht aktiviert haben.

Die folgenden Anweisungen gelten nur, wenn Sie die zentrale Konfiguration nicht verwenden.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten, um neue Steuerungen in aktivierten Standards automatisch zu aktivieren.

> **Note**
>
> Wenn Sie neue Steuerelemente mithilfe der folgenden Anweisungen automatisch aktivieren, können Sie unmittelbar nach der Veröffentlichung mit den Steuerelementen in der Konsole und programmgesteuert interagieren. Automatisch aktivierte Steuerelemente haben jedoch vorübergehend den Standardstatus Deaktiviert. Es kann mehrere Tage dauern, bis Security Hub CSPM die Kontrollfreigabe verarbeitet und die Kontrolle in Ihrem Konto als Aktiviert kennzeichnet. Während des Verarbeitungszeitraums können Sie eine Steuerung manuell aktivieren oder deaktivieren, und Security Hub CSPM behält diese Bezeichnung bei, unabhängig davon, ob Sie die automatische Steuerung aktiviert haben.

Security Hub CSPM console

Um neue Steuerungen automatisch zu aktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Allgemein aus.
3. Wählen Sie unter Steuerelemente die Option Bearbeiten aus.
4. Aktivieren Sie Auto-enable neue Steuerelemente in aktivierten Standards.
5. Wählen Sie Speichern.

Security Hub CSPM API

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie `UpdateSecurityHubConfiguration`.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, stellen Sie `AutoEnableControls` auf ein`true`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, legen Sie den Wert `AutoEnableControls` auf False fest.

AWS CLI

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie den Befehl `update-security-hub-configuration` aus.
2. Geben Sie Folgendes an, um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren`--auto-enable-controls`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, geben Sie Folgendes an`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Beispiel für einen Befehl

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Wenn Sie neue Steuerelemente nicht automatisch aktivieren, müssen Sie sie manuell aktivieren. Detaillierte Anweisungen finden Sie unter Steuerelemente in Security Hub CSPM aktivieren.

Deaktivieren der Steuerelemente in Security Hub CSPM

Um Störgeräusche bei der Suche zu vermeiden, kann es hilfreich sein, Steuerungen zu deaktivieren, die für Ihre Umgebung nicht relevant sind. In AWS Security Hub CSPM können Sie eine Steuerung für alle Sicherheitsstandards oder nur für bestimmte Standards deaktivieren.

Wenn Sie ein Steuerelement für alle Standards deaktivieren, passiert Folgendes:

- Sicherheitsüberprüfungen für das Steuerelement werden nicht mehr durchgeführt.
- Für die Kontrolle werden keine zusätzlichen Ergebnisse generiert.

- Bestehende Ergebnisse für die Kontrolle werden nicht mehr aktualisiert.
- Bestehende Ergebnisse für die Kontrolle werden automatisch archiviert, in der Regel innerhalb von 3—5 Tagen nach bestem Bemühen.
- Security Hub CSPM entfernt alle zugehörigen AWS Config Regeln, die es für die Kontrolle erstellt hat.

Wenn Sie ein Steuerelement nur für bestimmte Standards deaktivieren, beendet Security Hub CSPM die Ausführung von Sicherheitsprüfungen für das Steuerelement nur für diese Standards. Dadurch wird auch die Kontrolle aus den Berechnungen der Sicherheitsbewertung für jeden dieser Standards entfernt. Wenn die Steuerung in anderen Standards aktiviert ist, behält Security Hub CSPM die zugehörige AWS Config Regel bei, falls zutreffend, und führt weiterhin Sicherheitsprüfungen für die Steuerung für die anderen Standards durch. Security Hub CSPM bezieht die Steuerung auch in die Berechnung der Sicherheitsbewertung für jeden der anderen Standards mit ein, was sich auf Ihre zusammenfassende Sicherheitsbewertung auswirkt.

Wenn Sie einen Standard deaktivieren, werden alle Steuerelemente, die für den Standard gelten, automatisch für diesen Standard deaktiviert. In anderen Standards sind die Steuerelemente jedoch möglicherweise weiterhin aktiviert. Wenn Sie einen Standard deaktivieren, verfolgt Security Hub CSPM nicht, welche Steuerelemente für den Standard deaktiviert wurden. Wenn Sie denselben Standard später erneut aktivieren, werden daher alle für ihn geltenden Steuerelemente automatisch aktiviert. Hinweise zum Deaktivieren eines Standards finden Sie unter. Deaktivierung eines Standards

Das Deaktivieren einer Steuerung ist keine permanente Aktion. Angenommen, Sie deaktivieren ein Steuerelement und aktivieren dann einen Standard, der das Steuerelement enthält. Das Steuerelement wird dann für diesen Standard aktiviert. Wenn Sie einen Standard in Security Hub CSPM aktivieren, werden alle Steuerelemente, die für den Standard gelten, automatisch aktiviert. Informationen zur Aktivierung eines Standards finden Sie unter. Einen Standard aktivieren

Themen

- Standardübergreifendes Deaktivieren einer Steuerung
- Deaktivieren eines Steuerelements in einem bestimmten Standard
- Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM

Standardübergreifendes Deaktivieren einer Steuerung

Wir empfehlen, eine AWS Security Hub CSPM-Steuerung standardübergreifend zu deaktivieren, um die Abstimmung in Ihrem gesamten Unternehmen aufrechtzuerhalten. Wenn Sie ein Steuerelement nur in bestimmten Standards deaktivieren, erhalten Sie weiterhin Ergebnisse für das Steuerelement, sofern es in anderen Standards aktiviert ist.

Cross-standard Deaktivierung in mehreren Konten und Regionen

Um eine Sicherheitskontrolle für mehrere AWS-Konten Länder zu deaktivieren AWS-Regionen, müssen Sie die zentrale Konfiguration verwenden.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die bestimmte Steuerungen für alle aktivierten Standards deaktivieren. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten, Organisationseinheiten oder dem Stammverzeichnis zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können sich beispielsweise dafür entscheiden, alle AWS CloudTrail Steuerelemente in einer Organisationseinheit zu deaktivieren, und Sie können wählen, alle IAM-Steuerelemente in einer anderen Organisationseinheit zu deaktivieren. Der Grad der Granularität hängt von Ihren beabsichtigten Sicherheitszielen in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Kontrollen standardübergreifend deaktiviert, finden Sie unter. Konfigurationsrichtlinien erstellen und zuordnen

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um die Kontrollen in allen Standards außer dem Service-Managed Standard: zu verwalten. AWS Control Tower Die Steuerungen für diesen Standard sollten im AWS Control Tower Dienst konfiguriert werden.

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerelemente konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet festlegen. Self-managed Konten müssen die Steuerelemente in jeder Region separat konfigurieren.

Cross-standard Deaktivierung in einem einzelnen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto sind, können Sie Konfigurationsrichtlinien nicht verwenden, um Steuerelemente in mehreren Konten und Regionen zentral zu deaktivieren. Sie können jedoch eine Steuerung in einem einzelnen Konto und einer Region deaktivieren.

Security Hub CSPM console

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich die Option Steuerelemente aus.
3. Wählen Sie die Option neben einem Steuerelement aus.
4. Wählen Sie Steuerung deaktivieren. Diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist.
5. Wählen Sie einen Grund für die Deaktivierung des Steuerelements aus und bestätigen Sie, indem Sie auf Deaktivieren klicken.
6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Security Hub CSPM API

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Rufen Sie die ListStandardsControlAssociations API auf. Geben Sie eine Sicherheitskontroll-ID an.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Rufen Sie die BatchUpdateStandardsControlAssociations API auf. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Um Standard-ARNs abzurufen, führen Sie `DescribeStandards` den Befehl aus.

3. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
   v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}}]
   }
   ```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

AWS CLI

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Führen Sie den Befehl list-standards-control-associations aus. Geben Sie eine Sicherheitskontroll-ID ein.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

2. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Führen Sie den `describe-standards` Befehl aus, um Standard-ARNs abzurufen.

3. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

   ```
   aws securityhub  --region us-east-1 batch-update-standards-control-associations
    --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
    to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
   ```

```
"arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]'
```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Deaktivieren eines Steuerelements in einem bestimmten Standard

Sie können ein Steuerelement nur in bestimmten Sicherheitsstandards und nicht in allen Sicherheitsstandards deaktivieren. Wenn das Steuerelement für andere aktivierte Standards gilt, führt AWS Security Hub CSPM weiterhin Sicherheitsprüfungen für das Steuerelement durch, und Sie erhalten weiterhin Ergebnisse für das Steuerelement.

Wir empfehlen, den Aktivierungsstatus einer Kontrolle für alle aktivierten Standards, für die die Kontrolle gilt, abzustimmen. Informationen zur Deaktivierung eines Steuerelements für alle Standards, für die es gilt, finden Sie unter. Standardübergreifendes Deaktivieren einer Steuerung

Auf der Seite mit den Standarddetails können Sie auch Steuerelemente in bestimmten Standards deaktivieren. Sie müssen die Steuerelemente in bestimmten Standards in jedem AWS-Konto und separat deaktivieren AWS-Region. Wenn Sie ein Steuerelement in bestimmten Standards deaktivieren, wirkt sich dies nur auf das aktuelle Konto und die Region aus.

Wählen Sie Ihre bevorzugte Methode und folgen Sie diesen Schritten, um ein Steuerelement in einem oder mehreren bestimmten Standards zu deaktivieren.

Security Hub CSPM console

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
3. Wählen Sie ein Steuerelement aus.
4. Wählen Sie „Steuerung deaktivieren“. Diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist.
5. Geben Sie einen Grund für die Deaktivierung des Steuerelements an und bestätigen Sie, indem Sie Deaktivieren wählen.

Security Hub CSPM API

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie `ListSecurityControlDefinitions` den Befehl aus und geben Sie einen Standard-ARN ein, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Um einen Standard-ARN zu erhalten, führen Sie den Befehl aus `DescribeStandards`. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Führen Sie aus `ListStandardsControlAssociations` und geben Sie eine bestimmte Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Führen Sie `BatchUpdateStandardsControlAssociations`. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to environment"}]
   ```

```
}
```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie den `list-security-control-definitions` Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Um einen Standard-ARN zu erhalten, führen Sie den Befehl aus`describe-standards`. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. Führen Sie den `list-standards-control-associations` Befehl aus und geben Sie eine bestimmte Kontroll-ID an, um den aktuellen Aktivierungsstatus einer Steuerung in jedem Standard zurückzugeben.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

3. Führen Sie den Befehl `batch-update-standards-control-associations` aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.

4. Stellen Sie den `AssociationStatus` Parameter auf den Wert ein`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

   ```
   aws securityhub  --region us-east-1 batch-update-standards-control-
   associations --standards-control-association-updates '[{"SecurityControlId":
    "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
   foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
    "UpdatedReason": "Not applicable to environment"}]'
   ```

Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM

Wir empfehlen, einige AWS Security Hub CSPM-Steuerelemente zu deaktivieren, um das Suchgeräusch und die Nutzungskosten zu reduzieren.

Steuerungen, die globale Ressourcen verwenden

Einige AWS-Services unterstützen globale Ressourcen, was bedeutet, dass Sie von jeder Ressource aus auf die Ressource zugreifen könnenAWS-Region. Um Kosten zu sparenAWS Config, können Sie die Aufzeichnung globaler Ressourcen in allen Regionen außer einer Region deaktivieren. Nachdem Sie dies getan haben, führt Security Hub CSPM jedoch weiterhin Sicherheitsüberprüfungen in allen Regionen durch, in denen eine Kontrolle aktiviert ist, und berechnet Ihnen Gebühren auf der Grundlage der Anzahl der Prüfungen pro Konto pro Region. Um das Suchrauschen zu reduzieren und die Kosten für Security Hub CSPM zu senken, sollten Sie daher auch Kontrollen deaktivieren, die globale Ressourcen in allen Regionen betreffen, mit Ausnahme der Region, in der globale Ressourcen erfasst werden.

Wenn ein Steuerelement globale Ressourcen umfasst, aber nur in einer Region verfügbar ist, können Sie, wenn Sie es in dieser Region deaktivieren, keine Ergebnisse für die zugrunde liegende Ressource abrufen. In diesem Fall empfehlen wir, das Steuerelement aktiviert zu lassen. Wenn Sie die regionsübergreifende Aggregation verwenden, sollte die Region, in der das Steuerelement verfügbar ist, die Aggregationsregion oder eine der verknüpften Regionen sein. Die folgenden Steuerelemente beziehen sich auf globale Ressourcen, sind jedoch nur in einer einzigen Region verfügbar:

- Alle CloudFront Steuerelemente — Nur in der Region USA Ost (Nord-Virginia) verfügbar
- GlobalAccelerator.1— Nur in der Region USA West (Oregon) verfügbar
- Route53.2— Nur in der Region USA Ost (Nord-Virginia) verfügbar
- WAF.1, WAF.6, WAF.7, WAF.8 — Nur in der Region USA Ost (Nord-Virginia) verfügbar

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen

aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.
Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.
Weitere Informationen zur zentralen Konfiguration finden Sie unterGrundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Für Kontrollen, die einen periodischen Zeitplantyp haben, ist es erforderlich, sie in Security Hub CSPM zu deaktivieren, um eine Abrechnung zu verhindern. Die Einstellung des AWS Config Parameters `includeGlobalResourceTypes` auf `false` hat keinen Einfluss auf die regelmäßigen Security Hub CSPM-Steuerungen.

Die folgenden Security Hub CSPM-Steuerelemente verwenden globale Ressourcen:

- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

CloudTrail Steuerelemente zur Protokollierung

Das CloudTrail.2Steuerelement bewertet die Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von AWS CloudTrail Trail-Logs. Wenn Sie diese Pfade in einem zentralen Protokollierungskonto protokollieren, müssen Sie diese Steuerung nur für das Konto und den Ort aktivieren, AWS-Region an dem die zentrale Protokollierung stattfindet.

Wenn Sie die zentrale Konfiguration verwenden, wird der Aktivierungsstatus eines Steuerelements auf die Heimatregion und die verknüpften Regionen verteilt. Sie können ein Steuerelement nicht in einigen Regionen deaktivieren und in anderen aktivieren. In diesem Fall können Sie die Ergebnisse des CloudTrail.2 Steuerelements unterdrücken, um das Suchrauschen zu reduzieren.

CloudWatch Alarmsteuerungen

Wenn Sie Amazon GuardDuty für die Erkennung von Anomalien anstelle von CloudWatch Amazon-Alarmen bevorzugen, können Sie die folgenden Steuerungen deaktivieren, die sich auf CloudWatch Alarme konzentrieren:

- [CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
- [CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
- [CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind
- [CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
- [CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind
- [CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung
- [CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
- [CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind
- [CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration
- [CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
- [CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
- [CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
- [CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
- [CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

Grundlegendes zu Sicherheitsüberprüfungen und Bewertungen in Security Hub CSPM

Für jedes Steuerelement, das Sie aktivieren, führt AWS Security Hub CSPM Sicherheitsprüfungen durch. Eine Sicherheitsüberprüfung führt zu einem Ergebnis, das Ihnen Aufschluss darüber gibt, ob eine bestimmte AWS Ressource den in der Kontrolle enthaltenen Regeln entspricht.

Einige Prüfungen werden in regelmäßigen Abständen ausgeführt. Andere Prüfungen werden nur ausgeführt, wenn sich der Ressourcenstatus ändert. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Viele Sicherheitsüberprüfungen verwenden AWS Config verwaltete oder benutzerdefinierte Regeln, um die Konformitätsanforderungen festzulegen. Um diese Prüfungen durchzuführen, müssen Sie die Ressourcenaufzeichnung für die erforderlichen Ressourcen einrichten AWS Config und aktivieren. Weitere Informationen zur Einrichtung finden Sie AWS Config unterAktivierung und Konfiguration AWS Config für Security Hub CSPM. Eine Liste der AWS Config Ressourcen, die Sie für jeden Standard aufzeichnen müssen, finden Sie unterErforderlich AWS Config Ressourcen für Kontrollbefunde. Andere Steuerelemente verwenden benutzerdefinierte Lambda-Funktionen, die von Security Hub CSPM verwaltet werden und keine Voraussetzungen erfordern.

Während Security Hub CSPM Sicherheitsüberprüfungen durchführt, generiert es Ergebnisse und weist ihnen einen Compliance-Status zu. Weitere Informationen zum Compliance-Status finden Sie unter. Bewertung des Compliance-Status der CSPM-Ergebnisse von Security Hub

Security Hub CSPM verwendet den Compliance-Status von Kontrollfeststellungen, um einen allgemeinen Kontrollstatus zu ermitteln. Auf der Grundlage des Kontrollstatus berechnet Security Hub CSPM außerdem eine Sicherheitsbewertung für alle aktivierten Kontrollen und für bestimmte Standards. Weitere Informationen erhalten Sie unter the section called “Konformitätsstatus und Kontrollstatus” und the section called “Berechnung der Sicherheitswerte”.

Wenn Sie konsolidierte Kontrollergebnisse aktiviert haben, generiert Security Hub CSPM auch dann ein einziges Ergebnis, wenn eine Kontrolle mit mehr als einem Standard verknüpft ist. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Themen

- Erforderlich AWS Config Ressourcen für Kontrollbefunde
- Zeitplan für die Ausführung von Sicherheitsprüfungen
- Generierung und Aktualisierung von Kontrollergebnissen

- Bewertung des Konformitätsstatus und des Kontrollstatus
- Berechnung der Sicherheitswerte

Erforderlich AWS Config Ressourcen für Kontrollbefunde

> **Note**
>
> Wenn Sie Security Hub CSPM und Security Hub verwenden, wird die Konfiguration der Ressourcenaufzeichnung für Sie verwaltet. Security Hub erstellt einen serviceverknüpften Konfigurationsrekorder mit allen Ressourcen, die sich auf die in Security Hub CSPM unterstützten Kontrollen beziehen, AWS Config und ruft direkte Informationen zu diesen ab. Weitere Informationen finden Sie unter Verwenden des serviceverknüpften Konfigurationsrekorders.

In AWS Security Hub CSPM verwenden einige Steuerelemente dienstbezogene AWS Config Regeln, die Konfigurationsänderungen in Ihren Ressourcen erkennen. AWS Damit Security Hub CSPM genaue Ergebnisse für diese Kontrollen generiert, müssen Sie die Ressourcenaufzeichnung in aktivieren AWS Config und einschalten. AWS Config Informationen darüber, wie Security Hub CSPM AWS Config Regeln verwendet und wie sie aktiviert und konfiguriert werden AWS Config, finden Sie unter. Aktivierung und Konfiguration AWS Config für Security Hub CSPM Ausführliche Informationen zur Ressourcenaufzeichnung finden Sie unter Arbeiten mit dem Konfigurationsrekorder im AWS Config Entwicklerhandbuch.

Um genaue Kontrollergebnisse zu erhalten, müssen Sie die AWS Config Ressourcenaufzeichnung für aktivierte Steuerelemente mit einem durch Änderung ausgelösten Zeitplantyp aktivieren. Für einige Steuerelemente mit einem periodischen Zeitplan ist auch eine Ressourcenaufzeichnung erforderlich. Auf dieser Seite sind die erforderlichen Ressourcen für diese Security Hub CSPM-Steuerelemente aufgeführt.

Security Hub CSPM-Steuerungen können auf verwalteten AWS Config Regeln oder benutzerdefinierten Security Hub CSPM-Regeln basieren. Stellen Sie sicher, dass es keine AWS Identity and Access Management (IAM-) Richtlinien oder AWS Organizations verwalteten Richtlinien gibt, die AWS Config verhindern, dass Sie Ihre Ressourcen aufzeichnen dürfen. Die CSPM-Steuerungen von Security Hub werten Ressourcenkonfigurationen direkt aus und berücksichtigen keine AWS Organizations Richtlinien.

> **Note**
>
> AWS-Regionen Wenn ein Steuerelement nicht verfügbar ist, ist die entsprechende Ressource in nicht verfügbar. AWS Config Eine Liste dieser Grenzwerte finden Sie unterRegionale Beschränkungen der Security Hub CSPM-Steuerungen.

Themen

- Erforderliche Ressourcen für alle Security Hub CSPM-Steuerelemente
- Erforderliche Ressourcen für die AWS Standard für grundlegende bewährte Sicherheitsverfahren
- Erforderliche Ressourcen für die CIS AWS Maßstab für Stiftungen
- Erforderliche Ressourcen für den Standard NIST SP 800-53 Revision 5
- Erforderliche Ressourcen für den Standard NIST SP 800-171 Revision 2
- Erforderliche Ressourcen für PCI DSS v3.2.1
- Erforderliche Ressourcen für AWS Standard für Ressourcen-Tagging

Erforderliche Ressourcen für alle Security Hub CSPM-Steuerelemente

Damit Security Hub CSPM Ergebnisse für durch Änderungen ausgelöste Kontrollen generiert, die aktiviert sind und eine AWS Config Regel verwenden, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config In dieser Tabelle ist auch angegeben, mit welchen Kontrollen ein bestimmter Ressourcentyp bewertet wird. Ein einzelnes Steuerelement kann mehr als einen Ressourcentyp auswerten.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
		APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
	`AWS::ApiGateway::DomainName`	APIGateway.11
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1
	`AWS::AppConfig::ConfigurationProfile`	AppConfig.2
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::AppRunner::VpcConnector`	AppRunner.2
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	Batch.3 Batch.4
	`AWS::Batch::JobQueue`	Batch.1
	`AWS::Batch::SchedulingPolicy`	Batch.2

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Bedrock	`AWS::Bedrock::DataSource`	Bedrock.1
Amazon Grundgestein AgentCore	`AWS::BedrockAgentCore::BrowserCustom`	BedrockAgentCore.5 BedrockAgentCore.6
	`AWS::BedrockAgentCore::CodeInterpreterCustom`	BedrockAgentCore.7
	`AWS::BedrockAgentCore::Gateway`	BedrockAgentCore.2 BedrockAgentCore.4
	`AWS::BedrockAgentCore::Memory`	BedrockAgentCore.3
	`AWS::BedrockAgentCore::Runtime`	BedrockAgentCore.1
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15 CloudFront.16 CloudFront.17
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::CloudTrail::EventDataStore`	CloudTrail.11
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	`AWS::CodeBuild::ReportGroup`	CodeBuild.7
CodeGuru Amazon-Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
CodeGuru Amazon-Rezensent	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Amazon Connect Connect-Kunde	`AWS::CustomerProfiles::ObjectType`	Connect.1
	`AWS::Connect::Instance`	Connect.2
AWS DataSync	`AWS::DataSync::Task`	DataSync.1 DataSync.2
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2
	`AWS::DMS::Endpoint`	DMS.9 DMS.10 DMS.11 DMS.12

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6 DMS.13
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::DHCPOptions`	EC2.174

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25 EC2.170 EC2.175 EC2.181
	`AWS::EC2::NatGateway`	EC2.40

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41
	`AWS::EC2::NetworkInterface`	EC2.22 EC2.35 EC2.180
	`AWS::EC2::PrefixList`	EC2.176
	`AWS::EC2::RouteTable`	EC2.42
	`AWS::EC2::SecurityGroup`	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	`AWS::EC2::SnapshotBlockPublicAccess`	EC2.182
	`AWS::EC2::SpotFleet`	EC2.173

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::EC2::Subnet`	EC2.15 EC2.44 ElastiCache.7
	`AWS::EC2::TrafficMirrorFilter`	EC2.178
	`AWS::EC2::TrafficMirrorSession`	EC2.177
	`AWS::EC2::TrafficMirrorTarget`	EC2.179
	`AWS::EC2::TransitGateway`	EC2.23 EC2.52
	`AWS::EC2::TransitGatewayAttachment`	EC2.33
	`AWS::EC2::TransitGatewayRouteTable`	EC2.34
	`AWS::EC2::Volume`	EC2.3 EC2.45

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::EC2::VPC`	EC2.6 EC2.46
	`AWS::EC2::VPCBlockPublicAccessOptions`	EC2.172
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnection`	EC2.49
	`AWS::EC2::VPNConnection`	EC2.20 EC2.171 EC2.183
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::CapacityProvider`	ECS.19

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17 ECS.18 ECS.20 ECS.21
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
	`AWS::EFS::FileSystem`	EFS.7 EFS.8

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7
	`AWS::EKS::Nodegroup`	EKS.9
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector.1
	`AWS::FraudDetector::Label`	FraudDetector.2
	`AWS::FraudDetector::Outcome`	FraudDetector.3
	`AWS::FraudDetector::Variable`	FraudDetector.4
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
AWS Glue	`AWS::Glue::Job`	Glue.1 Glue.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWS IoT SiteWise	`AWS::IoTSiteWise::AssetModel`	IoTSiteWise.1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::IoTSiteWise::Dashboard`	IoTSiteWise.2
	`AWS::IoTSiteWise::Gateway`	IoTSiteWise.3
	`AWS::IoTSiteWise::Portal`	IoTSiteWise.4
	`AWS::IoTSiteWise::Project`	IoTSiteWise.5
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity`	IoTTwinMaker.4
	`AWS::IoTTwinMaker::Scene`	IoTTwinMaker.3
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWS IoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (für Apache Cassandra)	`AWS::Cassandra::Keyspace`	Keyspaces.1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MSK.5
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9 NetworkFirewall.10
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
		RDS.37 RDS.47 RDS.48
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	`AWS::RDS::DBSecurityGroup`	RDS.31
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
	`AWS::RDS::GlobalCluster`	RDS.51
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.10 Redshift.11 Redshift.18
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Redshift.17

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Redshift.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail.7 S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
	`AWS::S3::MultiRegionAccessPoint`	S3.24

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker KI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::InferenceExperiment`	SageMaker.23 SageMaker.24
	`AWS::SageMaker::Model`	SageMaker.5 SageMaker.16 SageMaker.19
	`AWS::SageMaker::ModelExplainabilityJobDefinition`	SageMaker.20
	`AWS::SageMaker::ModelQualityJobDefinition`	SageMaker.25
	`AWS::SageMaker::MonitoringSchedule`	SageMaker.22

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3 SageMaker.21
	`AWS::SageMaker::FeatureGroup`	SageMaker.17 SageMaker.18
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2 SES.3
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQS.3

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager (SSM)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transfer.4
	`AWS::Transfer::Certificate`	Transfer.5
	`AWS::Transfer::Connector`	Transfer.3 Transfer.6
	`AWS::Transfer::Profile`	Transfer.7
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces.1 WorkSpaces.2

Erforderliche Ressourcen für die AWS Standard für grundlegende bewährte Sicherheitsverfahren

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die den Standard „Best Practices von AWS Foundation Security“ (v.1.0.0) erfüllen, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM

AWS-Service	Ressourcentypen
Amazon API Gateway	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

AWS-Service	Ressourcentypen
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock	`AWS::Bedrock::DataSource`
Amazon Grundgestein AgentCore	`AWS::BedrockAgentCore::BrowserCustom` , `AWS::BedrockAgentCore::CodeInterpreterCustom` , `AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Runtime`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project` , `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool` , `AWS::Cognito::UserPool`
AWS CloudTrail	`AWS::CloudTrail::EventDataStore`
Amazon Connect Connect-Kunde	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

AWS-Service	Ressourcentypen
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::SnapshotBlockPublicAccess` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::CapacityProvider` , `AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition` , `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint` , `AWS::EFS::FileSystem`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::Nodegroup`

AWS-Service	Ressourcentypen
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

AWS-Service	Ressourcentypen
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBProxy` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription` , `AWS::RDS::GlobalCluster`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift Serverless	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket` , `AWS::S3::MultiRegionAccessPoint` , `AWS::S3Express::DirectoryBucket`
Amazon SageMaker KI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::InferenceExperiment` , `AWS::SageMaker::Model` , `AWS::SageMaker::ModelExplainabilityJobDefinition` , `AWS::SageMaker::ModelQualityJobDefinition` , `AWS::SageMaker::MonitoringSchedule` , `AWS::SageMaker::NotebookInstance`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`

AWS-Service	Ressourcentypen
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

Erforderliche Ressourcen für die CIS AWS Maßstab für Stiftungen

Um Sicherheitsüberprüfungen für aktivierte Kontrollen durchzuführen, die für den Center for Internet Security (CIS) AWS Foundations Benchmark gelten, führt Security Hub CSPM entweder genau die für die Prüfungen vorgeschriebenen Prüfschritte durch oder verwendet spezifische AWS Config verwaltete Regeln. Informationen zu diesem Standard in Security Hub CSPM finden Sie unter. CIS AWS Benchmark für Stiftungen im Security Hub CSPM

Erforderliche Ressourcen für CIS v5.0.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v5.0.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::FileSystem`

AWS-Service	Ressourcentypen
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance` , `AWS::RDS::DBCluster`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::Bucket`

Erforderliche Ressourcen für CIS v3.0.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v3.0.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::Bucket`

Erforderliche Ressourcen für CIS v1.4.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.4.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::Bucket`

Erforderliche Ressourcen für CIS v1.2.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.2.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Erforderliche Ressourcen für den Standard NIST SP 800-53 Revision 5

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die für den Standard NIST SP 800-53 Revision 5 gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. NIST SP 800-53 Revision 5 im Security Hub CSPM

AWS-Service	Ressourcentypen
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

AWS-Service	Ressourcentypen
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Grundgestein AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`

AWS-Service	Ressourcentypen
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

AWS-Service	Ressourcentypen
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

AWS-Service	Ressourcentypen
Amazon SageMaker KI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Erforderliche Ressourcen für den Standard NIST SP 800-171 Revision 2

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die für den Standard NIST SP 800-171 Revision 2 gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. NIST SP 800-171 Revision 2 im Security Hub CSPM

AWS-Service	Ressourcentypen
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`

AWS-Service	Ressourcentypen
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(ICH BIN)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Erforderliche Ressourcen für PCI DSS v3.2.1

Damit Security Hub CSPM die Ergebnisse für Kontrollen, die für Version 3.2.1 des Payment Card Industry Data Security Standard (PCI DSS) gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. PCI DSS im Security Hub CSPM

AWS-Service	Ressourcentypen
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`

AWS-Service	Ressourcentypen
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot`
Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon-S3)	`AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

Erforderliche Ressourcen für AWS Standard für Ressourcen-Tagging

Alle Steuerelemente, die für den AWS Resource Tagging-Standard gelten, werden durch Änderungen ausgelöst und verwenden eine AWS Config Regel. Damit Security Hub CSPM die Ergebnisse dieser Kontrollen korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. AWS Standard für Ressourcen-Tagging in Security Hub CSPM

AWS-Service	Ressourcentypen
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`

AWS-Service	Ressourcentypen
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::ConfigurationProfile` , `AWS::AppConfig::Environment` , `AWS::AppConfig::ExtensionAssociation`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` , `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan` , `AWS::Backup::BackupVault` , `AWS::Backup::RecoveryPlan` , `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment` , `AWS::Batch::JobQueue` , `AWS::Batch::SchedulingPolicy`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup` , `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS-Service	Ressourcentypen
Amazon Connect Connect-Kunde	`AWS::CustomerProfiles::ObjectType`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate` , `AWS::DMS::EventSubscription`
	
	`AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationSubnetGroup`

AWS DataSync	`AWS::DataSync::Task`
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway` , `AWS::EC2::DHCPOptions` , `AWS::EC2::EIP` , `AWS::EC2::FlowLog` , `AWS::EC2::Instance` , `AWS::EC2::InternetGateway` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NatGateway` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::PrefixList` , `AWS::EC2::RouteTable` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TrafficMirrorFilter` , `AWS::EC2::TrafficMirrorSession` , `AWS::EC2::TrafficMirrorTarget` , `AWS::EC2::TransitGateway` , `AWS::EC2::TransitGatewayAttachment` , `AWS::EC2::TransitGatewayRouteTable` , `AWS::EC2::Volume` , `AWS::EC2::VPC` , `AWS::EC2::VPCEndpointService` , `AWS::EC2::VPCPeeringConnection` , `AWS::EC2::VPNGateway`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`

AWS-Service	Ressourcentypen
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`

Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label`
	
	`AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`

AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`
Amazon GuardDuty	`AWS::GuardDuty::Detector` , `AWS::GuardDuty::Filter` , `AWS::GuardDuty::IPSet`
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Role` , `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer (IAM-Zugriffsanalysator)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`

AWS-Service	Ressourcentypen
AWS IoT Events	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoT Drahtlos	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (für Apache Cassandra)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

AWS-Service	Ressourcentypen
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSecurityGroup` , `AWS::RDS::DBSnapshot` , `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterParameterGroup` , `AWS::Redshift::ClusterSnapshot` , `AWS::Redshift::ClusterSubnetGroup` , `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
Amazon SageMaker KI	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` , `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager (SSM)	`AWS::SSM::Document`

AWS-Service	Ressourcentypen
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Zeitplan für die Ausführung von Sicherheitsprüfungen

Nachdem Sie einen Sicherheitsstandard aktiviert haben, beginnt AWS Security Hub CSPM, alle Prüfungen innerhalb von zwei Stunden durchzuführen. Die meisten Prüfungen beginnen innerhalb von 25 Minuten zu laufen. Security Hub CSPM führt Prüfungen durch, indem es die Regel auswertet, die einer Kontrolle zugrunde liegt. Bis ein Steuerelement seinen ersten Prüflauf abgeschlossen hat, lautet sein Status Keine Daten.

Wenn Sie einen neuen Standard aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe zugrunde liegende AWS Config serviceverknüpfte Regel verwenden wie aktivierte Steuerelemente aus anderen aktivierten Standards. Wenn Sie beispielsweise die Lambda.1Steuerung im Standard AWS Foundation Security Best Practices (FSBP) aktivieren, erstellt Security Hub CSPM die serviceverknüpfte Regel und generiert Ergebnisse in der Regel innerhalb von Minuten. Wenn Sie danach die Lambda.1 Steuerung im Payment Card Industry Data Security Standard (PCI DSS) aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM Ergebnisse für die Kontrolle generiert, da es dieselbe serviceverknüpfte Regel verwendet.

Nach der ersten Überprüfung kann der Zeitplan für jede Kontrolle entweder in regelmäßigen Abständen oder durch Änderungen ausgelöst werden. Für ein Steuerelement, das auf einer verwalteten AWS Config Regel basiert, enthält die Beschreibung des Steuerelements einen Link zur Regelbeschreibung im AWS ConfigEntwicklerhandbuch. Diese Beschreibung gibt an, ob es sich bei der Regel um eine Änderung handelt oder ob es sich um eine periodische Regel handelt

Regelmäßige Sicherheitsüberprüfungen

Regelmäßige Sicherheitsüberprüfungen werden automatisch innerhalb von 12 oder 24 Stunden nach der letzten Ausführung ausgeführt. Security Hub CSPM bestimmt die Periodizität, und Sie können sie nicht ändern. Bei regelmäßigen Kontrollen erfolgt die Bewertung zu dem Zeitpunkt, zu dem die Prüfung ausgeführt wird.

Wenn Sie den Workflow-Status eines periodischen Kontrollbefundes aktualisieren und dann bei der nächsten Überprüfung der Konformitätsstatus des Ergebnisses unverändert bleibt, bleibt der Workflow-Status in seinem geänderten Status. Wenn Sie beispielsweise eine fehlerhafte Suche für das KMS.4Steuerelement haben (AWS KMS keyRotation sollte aktiviert sein) und das Ergebnis anschließend korrigieren, ändert Security Hub CSPM den Workflow-Status von zu. `NEW` `RESOLVED` Wenn Sie die KMS-Schlüsselrotation vor der nächsten regelmäßigen Überprüfung deaktivieren, bleibt der Workflow-Status des Ergebnisses erhalten. `RESOLVED`

Prüfungen, die benutzerdefinierte Lambda-Funktionen von Security Hub CSPM verwenden, werden regelmäßig durchgeführt.

Change-triggered Sicherheitsüberprüfungen

Change-triggered Sicherheitsüberprüfungen werden ausgeführt, wenn sich der Status der zugehörigen Ressource ändert. AWS Configermöglicht es Ihnen, zwischen der kontinuierlichen Aufzeichnung von Änderungen des Ressourcenstatus und der täglichen Aufzeichnung zu wählen. Wenn Sie die tägliche Aufzeichnung wählenAWS Config, werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann die Generierung von Security Hub CSPM-Ergebnissen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist. Unabhängig von Ihrem gewählten Aufzeichnungszeitraum überprüft Security Hub CSPM mindestens einmal alle 24 Stunden, ob keine Ressourcen-Updates von verpasst AWS Config wurden.

Im Allgemeinen verwendet Security Hub CSPM, wann immer dies möglich ist, durch Änderungen ausgelöste Regeln. Damit eine Ressource eine durch Änderungen ausgelöste Regel verwenden kann, muss sie Konfigurationselemente unterstützen. AWS Config

Generierung und Aktualisierung von Kontrollergebnissen

AWSSecurity Hub CSPM generiert und aktualisiert Kontrollergebnisse, wenn es Prüfungen anhand von Sicherheitskontrollen durchführt. Die Kontrollergebnisse verwenden das AWSSecurity Finding Format (ASFF).

Security Hub CSPM berechnet normalerweise Gebühren für jede Sicherheitsüberprüfung für eine Kontrolle. Wenn jedoch mehrere Kontrollen dieselbe AWS Config Regel verwenden, berechnet Security Hub CSPM für jede Überprüfung anhand der Regel nur einmal eine Gebühr. Die AWS Config `iam-password-policy` Regel wird beispielsweise von mehreren Kontrollen im CIS AWS Foundations Benchmark-Standard und im AWS Foundational Security Best Practices-Standard verwendet. Jedes Mal, wenn Security Hub CSPM eine Prüfung anhand dieser Regel durchführt,

generiert es ein separates Kontrollergebnis für jede zugehörige Kontrolle, berechnet jedoch nur einmal für die Prüfung eine Gebühr.

Wenn die Größe eines Kontrollergebnisses das Maximum von 240 KB überschreitet, entfernt Security Hub CSPM das `Resource.Details` Objekt aus dem Befund. Bei Kontrollen, die durch AWS Config Ressourcen unterstützt werden, können Sie die Ressourcendetails mithilfe der AWS Config Konsole überprüfen.

Themen

- Konsolidierte Kontrollergebnisse
- Generierung, Aktualisierung und Archivierung von Kontrollbefunden
- Automatisierung und Unterdrückung von Kontrollbefunden
- Einzelheiten zur Einhaltung der Kontrollbestimmungen
- ProductFields Einzelheiten zu den Kontrollbefunden
- Schweregrade der Kontrollbefunde

Konsolidierte Kontrollergebnisse

Wenn konsolidierte Kontrollergebnisse für Ihr Konto aktiviert sind, generiert Security Hub CSPM für jede Sicherheitsüberprüfung einer Kontrolle ein einzelnes Ergebnis oder ein einzelnes Befundupdate, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt. Eine Liste der Kontrollen und der Standards, für die sie gelten, finden Sie unter. Kontrollreferenz für Security Hub CSPM Wir empfehlen, konsolidierte Kontrollergebnisse zu aktivieren, um das Störgeräusch zu reduzieren.

Wenn Sie Security Hub CSPM AWS-Konto vor dem 23. Februar 2023 aktiviert haben, können Sie konsolidierte Kontrollergebnisse aktivieren, indem Sie den Anweisungen weiter unten in diesem Abschnitt folgen. Wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren, werden die konsolidierten Kontrollergebnisse automatisch für Ihr Konto aktiviert.

Wenn Sie die Security Hub CSPM-Integration mit Mitgliedskonten verwenden AWS Organizations oder Mitgliedskonten über einen manuellen Einladungsprozess eingeladen haben, ist Consolidated Control Findings nur dann für Mitgliedskonten aktiviert, wenn sie für das Administratorkonto aktiviert ist. Wenn die Funktion für das Administratorkonto deaktiviert ist, ist sie auch für Mitgliedskonten deaktiviert. Dieses Verhalten gilt für neue und bestehende Mitgliedskonten. Wenn der Administrator die zentrale Konfiguration verwendet, um Security Hub CSPM für mehrere Konten zu verwalten, kann er außerdem keine zentralen Konfigurationsrichtlinien verwenden, um konsolidierte Kontrollergebnisse für die Konten zu aktivieren oder zu deaktivieren.

Wenn Sie konsolidierte Kontrollergebnisse für Ihr Konto deaktivieren, generiert oder aktualisiert Security Hub CSPM ein separates Kontrollergebnis für jeden aktivierten Standard, der eine Kontrolle enthält. Wenn Sie beispielsweise vier Standards aktivieren, die sich eine Kontrolle teilen, erhalten Sie nach einer Sicherheitsüberprüfung für die Kontrolle vier separate Ergebnisse. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis.

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erstellt Security Hub CSPM neue standardunabhängige Ergebnisse und archiviert die ursprünglichen standardbasierten Ergebnisse. Einige Felder und Werte für Kontrollergebnisse werden sich ändern, was sich auf Ihre bestehenden Workflows auswirken kann. Informationen zu diesen Änderungen finden Sie unterKonsolidierte Kontrollergebnisse — ASFF-Änderungen. Die Aktivierung konsolidierter Kontrollergebnisse kann sich auch auf die Ergebnisse auswirken, die integrierte Drittanbieterprodukte von Security Hub CSPM erhalten. Wenn Sie die Lösung Automated Security Response auf AWS Version 2.0.0 verwenden, beachten Sie, dass sie konsolidierte Kontrollergebnisse unterstützt.

Um Consolidated Control Findings zu aktivieren oder zu deaktivieren, müssen Sie mit einem Administratorkonto oder einem eigenständigen Konto angemeldet sein.

> **Note**
>
> Nachdem Sie die konsolidierten Kontrollergebnisse aktiviert haben, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM neue konsolidierte Ergebnisse generiert und die vorhandenen standardbasierten Ergebnisse archiviert hat. Ebenso kann es nach der Deaktivierung konsolidierter Kontrollergebnisse bis zu 24 Stunden dauern, bis Security Hub CSPM neue standardbasierte Ergebnisse generiert und die vorhandenen konsolidierten Ergebnisse archiviert hat. In diesen Zeiten kann es sein, dass Sie in Ihrem Konto eine Mischung aus standardunabhängigen und standardbasierten Ergebnissen sehen.

Security Hub CSPM console

Um konsolidierte Kontrollergebnisse zu aktivieren oder zu deaktivieren

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Klicken Sie im Navigationsbereich unter Settings auf General.
3. Wählen Sie im Bereich Steuerelemente die Option Bearbeiten aus.

4. Verwenden Sie den Schalter Konsolidierte Kontrollergebnisse, um konsolidierte Kontrollergebnisse zu aktivieren oder zu deaktivieren.
5. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie den UpdateSecurityHubConfigurationBetrieb der Security Hub CSPM-API, um konsolidierte Kontrollergebnisse programmgesteuert zu aktivieren oder zu deaktivieren. Oder, wenn Sie den verwenden, führen Sie den Befehl ausAWS CLI. update-security-hub-configuration

Geben Sie für den `control-finding-generator` Parameter `SECURITY_CONTROL` an, ob konsolidierte Kontrollergebnisse aktiviert werden sollen. Geben Sie an, um konsolidierte Kontrollergebnisse zu deaktivieren`STANDARD_CONTROL`.

Mit dem folgenden AWS CLI Befehl werden beispielsweise konsolidierte Kontrollbefunde aktiviert.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Mit dem folgenden AWS CLI Befehl werden konsolidierte Kontrollergebnisse deaktiviert.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Generierung, Aktualisierung und Archivierung von Kontrollbefunden

Security Hub CSPM führt Sicherheitsüberprüfungen nach einem Zeitplan durch. Wenn Security Hub CSPM zum ersten Mal eine Sicherheitsüberprüfung für ein Steuerelement durchführt, generiert es für jede AWS Ressource, die das Steuerelement überprüft, ein neues Ergebnis. Jedes Mal, wenn Security Hub CSPM anschließend eine Sicherheitsüberprüfung für die Kontrolle durchführt, aktualisiert es die vorhandenen Ergebnisse, um die Ergebnisse der Prüfung zu melden. Das bedeutet, dass Sie anhand der Daten einzelner Ergebnisse die Konformität bestimmter Ressourcen anhand bestimmter Kontrollen nachverfolgen können.

Wenn sich beispielsweise der Konformitätsstatus einer Ressource `PASSED` für eine bestimmte Kontrolle von `FAILED` zu ändert, generiert Security Hub CSPM kein neues Ergebnis. Stattdessen aktualisiert Security Hub CSPM die vorhandenen Ergebnisse für das Steuerelement und die

Ressource. In diesem Ergebnis ändert Security Hub CSPM den Wert für das Feld Compliance-Status (`Compliance.Status`) auf. `PASSED` Security Hub CSPM aktualisiert auch die Werte für zusätzliche Felder, um die Ergebnisse der Prüfung widerzuspiegeln, z. B. den Schweregrad, den Workflow-Status und Zeitstempel, die angeben, wann Security Hub CSPM die Prüfung zuletzt ausgeführt und das Ergebnis aktualisiert hat.

Bei der Meldung von Änderungen des Compliance-Status aktualisiert Security Hub CSPM möglicherweise eines der folgenden Felder in einem Kontrollergebnis:

- `Compliance.Status`— Der neue Konformitätsstatus der Ressource für die angegebene Kontrolle.
- `FindingProviderFields.Severity.Label`— Die neue qualitative Darstellung des Schweregrads des Befundes, z. B. `LOW`MEDIUM, oder`HIGH`.
- `FindingProviderFields.Severity.Original`— Die neue quantitative Darstellung des Schweregrads des Fehlers, z. B. `0` für eine konforme Ressource.
- `FirstObservedAt`— Wann sich der Konformitätsstatus der Ressource zuletzt geändert hat.
- `LastObservedAt`— Wann Security Hub CSPM die Sicherheitsüberprüfung für das angegebene Steuerelement und die angegebene Ressource zuletzt ausgeführt hat.
- `ProcessedAt`— Wann Security Hub CSPM zuletzt mit der Verarbeitung des Ergebnisses begann.
- `ProductFields.PreviousComplianceStatus`— Der vorherige Konformitätsstatus (`Compliance.Status`) der Ressource für die angegebene Kontrolle.
- `UpdatedAt`— Wann Security Hub CSPM das Ergebnis zuletzt aktualisiert hat.
- `Workflow.Status`— Der Stand der Untersuchung des Ergebnisses, basierend auf dem neuen Konformitätsstatus der Ressource für die angegebene Kontrolle.

Ob Security Hub CSPM ein Feld aktualisiert, hängt in erster Linie von den Ergebnissen der letzten Sicherheitsprüfung für die entsprechende Kontrolle und Ressource ab. Wenn sich beispielsweise der Konformitätsstatus einer Ressource `FAILED` für eine bestimmte Kontrolle von `PASSED` zu ändert, ändert Security Hub CSPM den Workflow-Status des Ergebnisses auf. `NEW` Um Aktualisierungen einzelner Ergebnisse nachzuverfolgen, können Sie auf die Historie eines Befundes zurückgreifen. Einzelheiten zu einzelnen Feldern in Ergebnissen finden Sie unter AWSSecurity Finding Format (ASFF).

In bestimmten Fällen generiert Security Hub CSPM neue Ergebnisse für nachfolgende Prüfungen durch eine Kontrolle, anstatt bestehende Ergebnisse zu aktualisieren. Dies kann der Fall sein, wenn ein Problem mit der AWS Config Regel vorliegt, die ein Steuerelement unterstützt. In diesem

Fall archiviert Security Hub CSPM den vorhandenen Befund und generiert für jede Prüfung einen neuen Befund. In den neuen Ergebnissen lautet der Compliance-Status `NOT_AVAILABLE` und der Datensatzstatus lautet. `ARCHIVED` Nachdem Sie das Problem mit der AWS Config Regel behoben haben, generiert Security Hub CSPM neue Ergebnisse und beginnt, diese zu aktualisieren, um nachfolgende Änderungen am Compliance-Status einzelner Ressourcen nachzuverfolgen.

Security Hub CSPM generiert und aktualisiert nicht nur Kontrollergebnisse, sondern archiviert auch automatisch Kontrollergebnisse, die bestimmte Kriterien erfüllen. Security Hub CSPM archiviert einen Befund, wenn das Steuerelement deaktiviert ist, die angegebene Ressource gelöscht wurde oder die angegebene Ressource nicht mehr existiert. Eine Ressource ist möglicherweise nicht mehr vorhanden, da der zugehörige Dienst nicht mehr verwendet wird. Insbesondere archiviert Security Hub CSPM automatisch ein Kontrollergebnis, wenn das Ergebnis eines der folgenden Kriterien erfüllt:

- Das Ergebnis wurde seit 3-5 Tagen nicht aktualisiert. Beachten Sie, dass die Archivierung auf der Grundlage dieses Zeitrahmens nach bestem Wissen und Gewissen erfolgt und nicht garantiert werden kann.
- `NOT_APPLICABLE`Bei der zugehörigen AWS Config Bewertung wurde der Konformitätsstatus der angegebenen Ressource ermittelt.

Um festzustellen, ob ein Ergebnis archiviert ist, können Sie im Feld Datensatzstatus (`RecordState`) des Ergebnisses nachschlagen. Wenn ein Ergebnis archiviert ist, lautet der Wert für dieses Feld`ARCHIVED`.

Security Hub CSPM speichert archivierte Kontrollergebnisse 30 Tage lang. Nach 30 Tagen laufen die Ergebnisse ab und Security Hub CSPM löscht sie dauerhaft. Um festzustellen, ob ein archiviertes Kontrollergebnis abgelaufen ist, stützt Security Hub CSPM seine Berechnung auf den Wert für das `UpdatedAt` Feld des Ergebnisses.

Um archivierte Kontrollergebnisse länger als 30 Tage zu speichern, können Sie die Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter Verwendung EventBridge für automatische Reaktionen und Problembehebungen.

> **Note**
>
> Vor dem 3. Juli 2025 generierte und aktualisierte Security Hub CSPM Kontrollergebnisse unterschiedlich, wenn sich der Compliance-Status einer Ressource für eine Kontrolle änderte. Zuvor hat Security Hub CSPM einen neuen Kontrollbefund erstellt und den vorhandenen

Befund für eine Ressource archiviert. Daher haben Sie möglicherweise mehrere archivierte Ergebnisse für eine bestimmte Kontrolle und Ressource, bis diese Ergebnisse ablaufen (nach 30 Tagen).

Automatisierung und Unterdrückung von Kontrollbefunden

Sie können die CSPM-Automatisierungsregeln von Security Hub verwenden, um bestimmte Kontrollergebnisse zu aktualisieren oder zu unterdrücken. Wenn Sie ein Ergebnis unterdrücken, können Sie weiterhin darauf zugreifen. Eine Unterdrückung deutet jedoch darauf hin, dass Sie der Ansicht sind, dass keine Maßnahmen erforderlich sind, um das Ergebnis zu beheben.

Durch das Unterdrücken von Ergebnissen können Sie das Suchrauschen reduzieren. Sie können beispielsweise Kontrollergebnisse unterdrücken, die in Testkonten generiert wurden. Oder Sie könnten Ergebnisse unterdrücken, die sich auf bestimmte Ressourcen beziehen. Weitere Informationen zur automatischen Aktualisierung oder Unterdrückung von Ergebnissen finden Sie unterGrundlegendes zu den Automatisierungsregeln in Security Hub CSPM.

Automatisierungsregeln eignen sich, wenn Sie bestimmte Kontrollergebnisse aktualisieren oder unterdrücken möchten. Wenn ein Steuerelement jedoch für Ihre Organisation oder Ihren Anwendungsfall nicht relevant ist, empfehlen wir, das Steuerelement zu deaktivieren. Wenn Sie eine Kontrolle deaktivieren, führt Security Hub CSPM keine Sicherheitsprüfungen für sie durch und es werden Ihnen keine Gebühren dafür berechnet.

Einzelheiten zur Einhaltung der Kontrollbestimmungen

Bei Ergebnissen, die durch Sicherheitsprüfungen für Kontrollen generiert wurden, enthalten das Compliance-Objekt und die Felder im AWS Security Finding Format (ASFF) Konformitätsdetails für einzelne Ressourcen, die von einer Kontrolle überprüft wurden. Dazu gehören die folgenden Informationen:

- `AssociatedStandards`— Die aktivierten Standards, in denen das Steuerelement aktiviert ist.
- `RelatedRequirements`— Die entsprechenden Anforderungen für die Steuerung in allen aktivierten Standards. Diese Anforderungen ergeben sich aus Sicherheits-Frameworks von Drittanbietern für die Steuerung, wie dem Payment Card Industry Data Security Standard (PCI DSS) oder dem Standard NIST SP 800-171 Revision 2.
- `SecurityControlId`— Die Kennung für die Steuerung aller Standards, die Security Hub CSPM unterstützt.

- `Status`— Das Ergebnis der letzten Überprüfung, die Security Hub CSPM für die Kontrolle durchgeführt hat. Die Ergebnisse früherer Prüfungen werden in der Befundhistorie gespeichert.
- `StatusReasons`— Ein Array, das die Gründe für den durch das `Status` Feld angegebenen Wert auflistet. Für jeden Grund enthält dies einen Ursachencode und eine Beschreibung.

In der folgenden Tabelle sind Ursachencodes und Beschreibungen aufgeführt, die ein Ergebnis in der `StatusReasons` Matrix enthalten könnte. Die Behebungsschritte hängen davon ab, welche Kontrolle ein Ergebnis mit einem bestimmten Ursachencode generiert hat. Die Anleitungen zur Problembehebung für eine Kontrolle finden Sie in der. Kontrollreferenz für Security Hub CSPM

Ursachencode	Compliance status (Compliance-Status)	Description
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	Für den CloudTrail Trail mit mehreren Regionen gibt es keinen gültigen metrischen Filter.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Metrische Filter sind für den Trail mit mehreren Regionen CloudTrail nicht vorhanden.
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	Das Konto verfügt nicht über einen CloudTrail Trail für mehrere Regionen mit der erforderlichen Konfiguration.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	Multi-Region CloudTrail Wanderwege befinden sich nicht in der aktuellen Region.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Es sind keine gültigen Alarmaktionen vorhanden.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch Alarme sind im Konto nicht vorhanden.

Ursachencode	Compliance status (Compliance-Status)	Description
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS ConfigStatus ist `ConfigError`	AWS ConfigZugriff verweigert. Stellen Sie sicher, dass es aktiviert AWS Config ist und dass ihm ausreichende Berechtigungen erteilt wurden.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Confighat Ihre Ressourcen anhand der Regel bewertet. Die Regel galt nicht für die AWS Ressourcen in ihrem Geltungsbereich, die angegebenen Ressourcen wurden gelöscht oder die Bewertungsergebnisse wurden gelöscht.
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(für Config.1)	Der AWS Config Rekorder verwendet eine benutzerdefinierte IAM-Rolle anstelle der AWS Config serviceverknüpften Rolle, und der `includeConfigServiceLinkedRoleCheck` benutzerdefinierte Parameter für Config.1 ist nicht auf festgelegt. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(für) Config.1	AWS Configist nicht aktiviert, wenn der Konfigurationsrekorder eingeschaltet ist.

Ursachencode	Compliance status (Compliance-Status)	Description
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(für Config.1)	AWS Configzeichnet nicht alle Ressourcentypen auf, die den aktivierten Security Hub CSPM-Steuerelementen entsprechen. Schalten Sie die Aufzeichnung für die folgenden Ressourcen ein:. *`Resources that aren't being recorded`*
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Der Konformitätsstatus ist darauf `NOT_AVAILABLE` zurückzuführen, dass der Status Nicht zutreffend AWS Config zurückgegeben wurde. AWS Configgibt keinen Grund für den Status an. Hier sind einige mögliche Gründe für den Status „Nicht zutreffend“: • Die Ressource wurde aus dem Geltungsbereich der AWS Config Regel entfernt. • Die AWS Config Regel wurde gelöscht. • Die Ressource wurde gelöscht. • Die AWS Config Regellogik kann den Status Nicht zutreffend erzeugen.

Ursachencode	Compliance status (Compliance-Status)	Description
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS ConfigDer Status ist `ConfigError`	Dieser Ursachencode wird für verschiedene Arten von Auswertungsfehlern verwendet. Die Beschreibung enthält die spezifischen Ursacheninformationen. Die Art des Fehlers kann einer der folgenden sein: • Unmöglichkeit, die Auswertung aufgrund fehlender Berechtigungen durchzuführen. Die Beschreibung enthält die spezifische Berechtigung, die fehlt. • Ein fehlender oder ungültiger Wert für einen Parameter. Die Beschreibung enthält den Parameter und die Anforderungen für den Parameterwert. • Fehler beim Lesen aus einem S3-Bucket. Die Beschreibung identifiziert den Bucket und stellt den spezifischen Fehler bereit. • Ein fehlendes AWS Abonnement. • Ein allgemeines Timeout für die Auswertung. • Ein gesperrtes Konto.

Ursachencode	Compliance status (Compliance-Status)	Description
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS ConfigStatus ist `ConfigError`	Die AWS Config Regel wird gerade erstellt.
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Es ist ein unbekannter Fehler aufgetreten.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	Security Hub CSPM kann keine Überprüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	Das Ergebnis befindet sich in einem `WARNING` Status, weil sich der S3-Bucket, der dieser Regel zugeordnet ist, in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Für die CloudWatch Logs-Metrikfilter gibt es kein gültiges Amazon SNS SNS-Abonnement.

Ursachencode	Compliance status (Compliance-Status)	Description
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Das Ergebnis befindet sich in einem WARNING Zustand. Das mit dieser Regel verknüpfte SNS-Thema gehört einem anderen Konto. Das aktuelle Konto kann die Abonnementinformationen nicht abrufen. Das Konto, dem das SNS-Thema gehört, muss dem aktuellen Konto die sns:ListSubscriptionsByTopic Berechtigung für das SNS-Thema gewähren.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Das Ergebnis weist einen WARNING Status auf, da sich das mit dieser Regel verknüpfte SNS-Thema in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
SNS_TOPIC_INVALID	FAILED	Das mit dieser Regel verknüpfte SNS-Thema ist ungültig.

Ursachencode	Compliance status (Compliance-Status)	Description
THROTTLING_ERROR	NOT_AVAILABLE	Die entsprechende API-Operation hat die zulässige Rate überschritten.

ProductFields Einzelheiten zu den Kontrollbefunden

Bei Ergebnissen, die bei Sicherheitsprüfungen für Kontrollen generiert wurden, kann das ProductFieldsAttribut im AWS Security Finding Format (ASFF) die folgenden Felder enthalten.

`ArchivalReasons:0/Description`

Beschreibt, warum Security Hub CSPM einen Befund archiviert hat.

Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren oder wenn Sie konsolidierte Kontrollergebnisse aktivieren oder deaktivieren.

`ArchivalReasons:0/ReasonCode`

Gibt an, warum Security Hub CSPM einen Befund archiviert hat.

Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren oder wenn Sie konsolidierte Kontrollergebnisse aktivieren oder deaktivieren.

`PreviousComplianceStatus`

Der vorherige Konformitätsstatus (`Compliance.Status`) der Ressource für die angegebene Kontrolle, zum Zeitpunkt der letzten Aktualisierung des Ergebnisses. Wenn sich der Konformitätsstatus der Ressource während der letzten Aktualisierung nicht geändert hat, entspricht dieser Wert dem Wert für das `Compliance.Status` Ergebnisfeld. Eine Liste möglicher Werte finden Sie unter Bewertung des Konformitätsstatus und des Kontrollstatus.

`StandardsGuideArn` oder `StandardsArn`

Der ARN des Standards, der dem Steuerelement zugeordnet ist.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld`StandardsGuideArn`. Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld. `StandardsArn`

Diese Felder werden zugunsten von entfernt, `Compliance.AssociatedStandards` wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`StandardsGuideSubscriptionArn` oder `StandardsSubscriptionArn`

Der ARN des Standardabonnements des Kontos.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld`StandardsGuideSubscriptionArn`. Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld. `StandardsSubscriptionArn`

Diese Felder werden entfernt, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`RuleId` oder `ControlId`

Der Bezeichner für das Steuerelement.

Für Version 1.2.0 des CIS AWS Foundations Benchmark-Standards lautet `RuleId` das Feld. Für andere Standards, einschließlich nachfolgender Versionen des Benchmark-Standards der CIS AWS Foundations, lautet das Feld`ControlId`.

Diese Felder werden zugunsten von entfernt, `Compliance.SecurityControlId` wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`RecommendationUrl`

Die URL mit Behebungsinformationen für das Steuerelement. Dieses Feld wird entfernt, `Remediation.Recommendation.Url` wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`RelatedAWSResources:0/name`

Der Name der Ressource, die dem Ergebnis zugeordnet ist.

`RelatedAWSResource:0/type`

Der Typ der Ressource, die dem Steuerelement zugeordnet ist.

`StandardsControlArn`

Der ARN des Steuerelements. Dieses Feld wird entfernt, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`aws/securityhub/ProductName`

Für Kontrollergebnisse lautet der Produktname`Security Hub`.

`aws/securityhub/CompanyName`

Für Kontrollergebnisse lautet der Firmenname`AWS`.

`aws/securityhub/annotation`

Eine Beschreibung des bei der Kontrolle aufgedeckten Problems.

`aws/securityhub/FindingId`

Die Kennung für den Befund.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Schweregrade der Kontrollbefunde

Der Schweregrad, der einer Security Hub-CSPM-Steuerung zugewiesen wurde, weist auf die Wichtigkeit der Kontrolle hin. Der Schweregrad einer Kontrolle bestimmt den Schweregrad, der den Kontrollergebnissen zugewiesen wird.

Schweregradkriterien

Der Schweregrad einer Kontrolle wird anhand der folgenden Kriterien bestimmt:

- Wie schwierig ist es für einen Bedrohungsakteur, die mit der Kontrolle verbundene Konfigurationsschwäche auszunutzen? Die Schwierigkeit wird durch den Grad an Raffinesse oder Komplexität bestimmt, der erforderlich ist, um die Schwachstelle zur Ausführung eines Bedrohungsszenarios auszunutzen.
- Wie wahrscheinlich ist es, dass die Schwachstelle zu einer Beeinträchtigung Ihrer Ressourcen AWS-Konten oder Ihrer Ressourcen führt? Eine Beeinträchtigung Ihrer AWS-Konten Ressourcen bedeutet, dass die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Daten oder AWS Infrastruktur in irgendeiner Weise beeinträchtigt wird. Die Wahrscheinlichkeit einer Gefährdung gibt an, wie wahrscheinlich es ist, dass das Bedrohungsszenario zu einer Störung oder einem Angriff auf Ihre Ressourcen AWS-Services oder Ihre Ressourcen führt.

Betrachten Sie als Beispiel die folgenden Konfigurationsschwächen:

- Benutzerzugriffsschlüssel werden nicht alle 90 Tage ausgetauscht.
- Der IAM-Root-Benutzerschlüssel ist vorhanden.

Beide Schwächen sind für einen Gegner gleichermaßen schwer auszunutzen. In beiden Fällen kann der Angreifer Anmeldeinformationen stehlen oder eine andere Methode verwenden, um an einen Benutzerschlüssel zu gelangen. Er kann es dann verwenden, um auf unautorisierte Weise auf Ihre Ressourcen zuzugreifen.

Die Wahrscheinlichkeit einer Kompromittierung ist jedoch viel höher, wenn der Bedrohungsakteur den Root-Benutzerzugriffsschlüssel erwirbt, da er dadurch besseren Zugriff hat. Infolgedessen hat die Schwäche des Root-Benutzerschlüssels einen höheren Schweregrad.

Der Schweregrad berücksichtigt nicht die Wichtigkeit der zugrunde liegenden Ressource. Kritikalität ist der Grad der Wichtigkeit der Ressourcen, die mit dem Ergebnis verknüpft sind. Beispielsweise ist eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, kritischer als eine, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das `Criticality` Feld des AWS Security Finding Formats (ASFF), um Informationen zur Ressourcenkritik zu erfassen.

In der folgenden Tabelle werden die Sicherheitslabel den Schwierigkeiten bei der Ausnutzung und der Wahrscheinlichkeit einer Gefährdung zugeordnet.

	Ein Kompromiss ist sehr wahrscheinlich	Kompromiss wahrscheinlich	Ein Kompromiss ist unwahrscheinlich	Ein Kompromiss ist höchst unwahrscheinlich
Sehr einfach auszunutzen	Kritisch	Kritisch	Hoch	Mittel
Etwas einfach auszunutzen	Kritisch	Hoch	Mittel	Mittel
Etwas schwer auszunutzen	Hoch	Mittel	Mittel	Niedrig
Sehr schwer auszunutzen	Mittel	Mittel	Niedrig	Niedrig

Schweregraddefinitionen

Die Schweregrade sind wie folgt definiert.

Kritisch — Das Problem sollte sofort behoben werden, um eine Eskalation zu vermeiden.

Beispielsweise wird ein offener S3-Bucket mit kritischem Schweregrad bewertet. Da so viele Bedrohungsakteure nach offenen S3-Buckets suchen, ist es wahrscheinlich, dass Daten in exponierten S3-Buckets von anderen entdeckt und abgerufen werden.

Im Allgemeinen gelten öffentlich zugängliche Ressourcen als kritische Sicherheitslücken. Sie sollten kritische Ergebnisse mit äußerster Dringlichkeit behandeln. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Hoch — Das Problem muss als kurzfristige Priorität angegangen werden.

Wenn eine Standard-VPC-Sicherheitsgruppe beispielsweise für eingehenden und ausgehenden Datenverkehr geöffnet ist, wird sie als hochgradig eingestuft. Für einen Bedrohungsakteur ist es ziemlich einfach, eine VPC mit dieser Methode zu kompromittieren. Es ist auch wahrscheinlich, dass der Bedrohungsakteur in der Lage sein wird, Ressourcen zu unterbrechen oder zu exfiltrieren, sobald sie sich in der VPC befinden.

Security Hub CSPM empfiehlt, dass Sie einen Befund mit hohem Schweregrad als kurzfristige Priorität behandeln. Sie sollten sofort Abhilfemaßnahmen ergreifen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Mittel — Das Problem sollte als mittelfristige Priorität angegangen werden.

Mangelnde Verschlüsselung für Daten bei der Übertragung wird beispielsweise als mittelgradig eingestuft. Um diese Schwachstelle auszunutzen, ist ein ausgeklügelter Man-in-the-Middle-Angriff erforderlich. Mit anderen Worten, es ist etwas schwierig. Es ist wahrscheinlich, dass einige Daten gefährdet werden, wenn das Bedrohungsszenario erfolgreich ist.

Security Hub CSPM empfiehlt, dass Sie die betroffene Ressource so schnell wie möglich untersuchen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Niedrig — Für das Problem sind keine eigenständigen Maßnahmen erforderlich.

Beispielsweise wird das Versäumnis, forensische Informationen zu sammeln, als niedriger Schweregrad angesehen. Diese Kontrolle kann dazu beitragen, future Kompromisse zu verhindern, aber das Fehlen von Forensik führt nicht direkt zu einem Kompromiss.

Bei Problemen mit geringem Schweregrad müssen Sie nicht sofort Maßnahmen ergreifen, sie können jedoch Kontext bieten, wenn Sie sie mit anderen Problemen korrelieren.

Informativ — Es wurde keine Sicherheitslücke in der Konfiguration gefunden.

Mit anderen Worten, der Status ist `PASSED`WARNING, oder`NOT AVAILABLE`.

Es gibt keine empfohlene Aktion. Informationsergebnisse helfen Kunden dabei, nachzuweisen, dass sie sich in einem konformen Zustand befinden.

Bewertung des Konformitätsstatus und des Kontrollstatus

Das `Compliance.Status` Feld des AWS Security Finding Formats beschreibt das Ergebnis eines Kontrollbefundes. AWSSecurity Hub CSPM verwendet den Compliance-Status von Kontrollfeststellungen, um einen allgemeinen Kontrollstatus zu ermitteln. Der Kontrollstatus wird auf der Detailseite einer Kontrolle in der Security Hub CSPM-Konsole angezeigt.

Bewertung des Compliance-Status der CSPM-Ergebnisse von Security Hub

Dem Konformitätsstatus für jedes Ergebnis wird einer der folgenden Werte zugewiesen:

- `PASSED`— Zeigt an, dass das Steuerelement die Sicherheitsüberprüfung für den Befund bestanden hat. Dadurch wird der Security Hub CSPM `Workflow.Status` automatisch auf eingestellt. `RESOLVED`
- `FAILED`— Zeigt an, dass das Steuerelement die Sicherheitsüberprüfung für das Ergebnis nicht bestanden hat.
- `WARNING`— Weist darauf hin, dass Security Hub CSPM nicht feststellen kann, ob sich die Ressource im Status „`PASSED`oder`FAILED`“ befindet. Beispielsweise ist die AWS ConfigRessourcenaufzeichnung für den entsprechenden Ressourcentyp nicht aktiviert.
- `NOT_AVAILABLE`— Zeigt an, dass die Prüfung nicht abgeschlossen werden kann, weil ein Server ausgefallen ist, die Ressource gelöscht wurde `NOT_APPLICABLE` oder das Ergebnis der AWS Config Auswertung Wenn das AWS Config Evaluierungsergebnis war`NOT_APPLICABLE`, archiviert Security Hub CSPM den Befund automatisch.

Wenn sich der Compliance-Status für ein Ergebnis von `PASSED` zu`FAILED`, oder `WARNING`NOT_AVAILABLE, ändert und `Workflow.Status` entweder `NOTIFIED` oder lautet`RESOLVED`, wechselt `Workflow.Status` Security Hub CSPM automatisch zu. `NEW`

Wenn Sie nicht über Ressourcen verfügen, die einer Kontrolle entsprechen, generiert Security Hub CSPM einen `PASSED` Befund auf Kontoebene. Wenn Sie über eine Ressource verfügen, die einem Steuerelement entspricht, die Ressource dann aber löschen, erstellt Security Hub CSPM einen `NOT_AVAILABLE` Befund und archiviert ihn sofort. Nach 18 Stunden erhalten Sie einen `PASSED` Befund, da Sie nicht mehr über Ressourcen verfügen, die der Kontrolle entsprechen.

Ableitung des Kontrollstatus aus dem Compliance-Status

Security Hub CSPM leitet aus dem Compliance-Status der Kontrollfeststellungen einen allgemeinen Kontrollstatus ab. Bei der Bestimmung des Kontrollstatus ignoriert Security Hub CSPM Ergebnisse mit einem `RecordState` von `ARCHIVED` und Ergebnisse mit einem von. `Workflow.Status` `SUPPRESSED`

Dem Kontrollstatus wird einer der folgenden Werte zugewiesen:

- Bestanden — Zeigt an, dass alle Ergebnisse den Konformitätsstatus haben`PASSED`.
- Fehlgeschlagen — Zeigt an, dass mindestens ein Ergebnis den Konformitätsstatus hat`FAILED`.
- Unbekannt — Gibt an, dass mindestens ein Ergebnis den Konformitätsstatus `WARNING` oder hat`NOT_AVAILABLE`. Keine Ergebnisse haben den Konformitätsstatus`FAILED`.
- Keine Daten — Zeigt an, dass keine Ergebnisse für die Kontrolle vorliegen. Beispielsweise hat ein neu aktiviertes Steuerelement diesen Status, bis Security Hub CSPM beginnt, Ergebnisse dafür zu generieren. Ein Steuerelement hat diesen Status auch, wenn alle seine Ergebnisse aktuell nicht verfügbar sind `SUPPRESSED` oder nicht verfügbar sind. AWS-Region
- Deaktiviert — Zeigt an, dass das Steuerelement im aktuellen Konto und in der Region deaktiviert ist. Für dieses Steuerelement werden derzeit keine Sicherheitsüberprüfungen im Girokonto und in der Region durchgeführt. Die Ergebnisse einer deaktivierten Kontrolle können sich jedoch bis zu 24 Stunden nach der Deaktivierung auf den Compliance-Status auswirken.

Bei einem Administratorkonto spiegelt der Kontrollstatus den Kontrollstatus für das Administratorkonto und die Mitgliedskonten wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlerhafte Ergebnisse im Administratorkonto oder in einem der Mitgliedskonten gefunden wurden. Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt der Kontrollstatus in der Aggregationsregion den Kontrollstatus in der Aggregationsregion und den verknüpften Regionen wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlgeschlagene Ergebnisse in der Aggregationsregion oder einer der verknüpften Regionen vorliegen.

Security Hub CSPM generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Sie müssen die AWS ConfigRessourcenaufzeichnung konfiguriert haben, damit der Kontrollstatus angezeigt wird. Nachdem die Kontrollstatus zum ersten Mal generiert wurden, aktualisiert Security Hub CSPM die Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse der letzten 24 Stunden. Ein Zeitstempel auf der Seite mit den Kontrolldetails gibt an, wann der Kontrollstatus zuletzt aktualisiert wurde.

> **Note**
>
> Nach der ersten Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis Kontrollstatus in den Regionen China und den AWS GovCloud (US) Region generiert werden.

Berechnung der Sicherheitswerte

Auf der AWS Security Hub CSPM-Konsole wird auf den Seiten „Zusammenfassung“ und „Kontrollen“ eine Zusammenfassung der Sicherheitsbewertung aller Ihrer aktivierten Standards angezeigt. Auf der Seite Sicherheitsstandards zeigt Security Hub CSPM außerdem für jeden aktivierten Standard eine Sicherheitsbewertung zwischen 0 und 100 Prozent an.

Wenn Sie Security Hub CSPM zum ersten Mal aktivieren, berechnet Security Hub CSPM die zusammenfassende Sicherheitsbewertung und die Standardsicherheitsbewertungen innerhalb von 30 Minuten nach Ihrem ersten Besuch der Seite „Zusammenfassung“ oder „Sicherheitsstandards“ auf der Konsole. Bewertungen werden nur für Standards generiert, die aktiviert werden, wenn Sie diese Seiten auf der Konsole aufrufen. Außerdem muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. Die zusammenfassende Sicherheitsbewertung ist der Durchschnitt der Standardsicherheitsbewertungen. Um eine Liste der derzeit aktivierten Standards zu überprüfen, können Sie den GetEnabledStandards Betrieb der Security Hub CSPM-API verwenden.

Nach der ersten Ergebnisgenerierung aktualisiert Security Hub CSPM die Sicherheitsbewertungen alle 24 Stunden. Security Hub CSPM zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde. Beachten Sie, dass es in den Regionen China und bis zu 24 Stunden dauern kann, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Regions

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, kann es bis zu 24 Stunden dauern, bis Ihre Sicherheitsbewertungen aktualisiert werden. Darüber hinaus werden vorhandene

Sicherheitsbewertungen zurückgesetzt, wenn Sie eine neue Aggregationsregion aktivieren oder verknüpfte Regionen aktualisieren. Es kann bis zu 24 Stunden dauern, bis Security Hub CSPM neue Sicherheitsbewertungen generiert, die Daten aus den aktualisierten Regionen enthalten.

Methode zur Berechnung der Sicherheitswerte

Die Sicherheitswerte stellen das Verhältnis der bestandenen Kontrollen zu den aktivierten Kontrollen dar. Die Punktzahl wird als Prozentsatz angezeigt, der auf die nächste ganze Zahl auf- oder abgerundet wird.

Security Hub CSPM berechnet eine Zusammenfassung der Sicherheitsbewertung für alle von Ihnen aktivierten Standards. Security Hub CSPM berechnet auch eine Sicherheitsbewertung für jeden aktivierten Standard. Zur Berechnung der Punktzahl gehören zu den aktivierten Kontrollen auch Kontrollen mit dem Status „Bestanden“, „Fehlgeschlagen“ und „Unbekannt“. Kontrollen mit dem Status Keine Daten sind von der Punkteberechnung ausgeschlossen.

Security Hub CSPM ignoriert archivierte und unterdrückte Ergebnisse bei der Berechnung des Kontrollstatus. Dies kann sich auf die Sicherheitsbewertungen auswirken. Wenn Sie beispielsweise alle Fehlschläge für eine Kontrolle unterdrücken, wird ihr Status in Bestanden geändert, was wiederum Ihre Sicherheitswerte verbessern kann. Weitere Informationen zum Kontrollstatus finden Sie unterBewertung des Konformitätsstatus und des Kontrollstatus.

Beispiel für eine Bewertung:

Standard	Kontrollen bestanden	Fehlgeschlagene Kontrollen	Unbekannte Steuerelemente	Standardpunktzahl
AWS Grundlegende bewährte Sicherheitsmethoden v1.0.0	168	22	0	88%
Benchmark v1.4.0 für die AWS CIS-Grundlagen	8	29	0	22%
Benchmark v1.2.0 für die	6	35	0	15%

Standard	Kontrollen bestanden	Fehlgeschlagene Kontrollen	Unbekannte Steuerelemente	Standardpunktzahl
AWS CIS-Grundlagen				
NIST-Sonderveröffentlichung 800-53 Revision 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Bei der Berechnung der Sicherheitsbewertung zählt Security Hub CSPM jede Kontrolle standardübergreifend nur einmal. Wenn Sie beispielsweise ein Steuerelement aktiviert haben, das für drei aktivierte Standards gilt, zählt es für Bewertungszwecke nur als ein aktiviertes Steuerelement.

In diesem Beispiel zählt Security Hub CSPM jedes einzelne Steuerelement zu Bewertungszwecken nur einmal, obwohl die Gesamtzahl der aktivierten Kontrollen in allen aktivierten Standards 528 beträgt. Die Anzahl der einzelnen aktivierten Steuerelemente liegt wahrscheinlich unter 528. Wenn wir davon ausgehen, dass die Anzahl der eindeutig aktivierten Steuerelemente 515 und die Anzahl der eindeutig übergebenen Kontrollen 357 beträgt, beträgt die Gesamtpunktzahl 69%. Dieser Wert wird berechnet, indem die Anzahl der eindeutig bestandenen Kontrollen durch die Anzahl der eindeutig aktivierten Kontrollen geteilt wird.

Möglicherweise haben Sie eine Gesamtbewertung, die von der Standardsicherheitsbewertung abweicht, auch wenn Sie in Ihrem Konto in der aktuellen Region nur einen Standard aktiviert haben. Dies kann vorkommen, wenn Sie mit einem Administratorkonto angemeldet sind und für Mitgliedskonten zusätzliche oder andere Standards aktiviert sind. Dies kann auch der Fall sein, wenn Sie das Ergebnis in der Aggregationsregion anzeigen und in verknüpften Regionen zusätzliche Standards oder andere Standards aktiviert sind.

Sicherheitsbewertungen für Administratorkonten

Wenn Sie mit einem Administratorkonto angemeldet sind, berücksichtigen die zusammenfassende Sicherheitsbewertung und die Standardbewertungen den Kontrollstatus im Administratorkonto und in allen Mitgliedskonten.

Wenn eine Kontrolle auch nur in einem Mitgliedskonto den Status Fehlgeschlagen hat, lautet ihr Status im Administratorkonto nicht bestanden, was sich auf die Ergebnisse des Administratorkontos auswirkt.

Wenn Sie mit einem Administratorkonto angemeldet sind und Ergebnisse in einer Aggregationsregion anzeigen, berücksichtigen die Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Sicherheitsbewertungen, wenn Sie eine Aggregationsregion festgelegt haben

Wenn Sie eine Aggregation festgelegt haben AWS-Region, berücksichtigen die zusammenfassende Sicherheitsbewertung und die Standardbewertungen den Kontrollstatus in allen verknüpfte Regionen.

Wenn der Status einer Steuerung auch nur in einer verknüpften Region „Fehlgeschlagen“ lautet, lautet ihr Status in der Aggregationsregion „Fehlgeschlagen“ und wirkt sich auf die Werte der Aggregationsregion aus.

Wenn Sie mit einem Administratorkonto angemeldet sind und Ergebnisse in einer Aggregationsregion anzeigen, berücksichtigen Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Kontrollkategorien in Security Hub CSPM

Jedem Steuerelement wird eine Kategorie zugewiesen. Die Kategorie einer Kontrolle spiegelt die Sicherheitsfunktion wider, auf die die Kontrolle angewendet wird.

Der Kategoriewert enthält die Kategorie, die Unterkategorie innerhalb der Kategorie und optional einen Klassifikator innerhalb der Unterkategorie. Beispiel:

- Identifizieren > Inventar
- Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Hier finden Sie die Beschreibungen der verfügbaren Kategorien, Unterkategorien und Klassifikatoren.

Identifizieren

Entwickeln Sie die organisatorische Grundlagen für das Management von Cybersicherheitsrisiken für Systeme, Assets, Daten und Funktionen.

Bestand

Hat der Service die richtigen Ressourcen-Tagging-Strategien implementiert? Schließen die Tagging-Strategien den Ressourcenbesitzer ein?

Welche Ressourcen werden vom Service genutzt? Sind sie für diesen Service genehmigte Ressourcen?

Haben Sie Einblick in den genehmigten Bestand? Verwenden Sie beispielsweise Dienste wie Amazon EC2 Systems Manager und Service Catalog?

Protokollierung

Haben Sie die gesamte relevante Protokollierung für den Service sicher aktiviert? Zu den Beispielen für Protokolldateien gehören die folgenden:

- Amazon-VPC-Flow-Protokolle
- Zugriffsprotokolle für Elastic Load Balancing
- CloudFront Amazon-Protokolle
- CloudWatch Amazon-Protokolle
- Protokollierung durch Amazon Relational Database Service
- Langsame Indexprotokolle von Amazon OpenSearch Service
- X-Ray Rückverfolgung
- AWS Directory ServiceLogs
- AWS ConfigArtikel
- -Snapshots

Schutz

Entwicklung und Implementierung geeigneter Sicherheitsvorkehrungen, um die Bereitstellung kritischer Infrastrukturservices und sicherer Codierungspraktiken zu gewährleisten.

Sichere Zugriffsverwaltung

Verwendet der Service in seinen IAM- oder Ressourcenrichtlinien Verfahren mit den geringsten Rechten?

Sind Passwörter und Secrets ausreichend komplex? Werden sie angemessen rotiert?

Verwendet der Service Multi-Factor Authentication (MFA)?

Vermeidet der Dienst den Root-Benutzer?

Erlauben ressourcenbasierte Richtlinien den öffentlichen Zugriff?

Sichere Netzwerkkonfiguration

Vermeidet der Service öffentlichen und unsicheren Remote-Netzwerkzugriff?

Verwendet der Service VPCs ordnungsgemäß? Müssen beispielsweise Aufträge in VPCs ausgeführt werden?

Segmentiert und isoliert der Service sensible Ressourcen ordnungsgemäß?

Datenschutz

Verschlüsselung von Daten im Ruhezustand — Verschlüsselt der Dienst Daten im Ruhezustand?

Verschlüsselung von Daten bei der Übertragung — Verschlüsselt der Dienst Daten bei der Übertragung?

Datenintegrität — Validiert der Dienst Daten auf Integrität?

Schutz vor Datenlöschung — Schützt der Dienst Daten vor versehentlichem Löschen?

Datenverwaltung/-nutzung — Verwenden Sie Dienste wie Amazon Macie, um den Standort Ihrer sensiblen Daten zu verfolgen?

API-Schutz

Wird der Service AWS PrivateLink zum Schutz der Service-API-Operationen verwendet?

Schutzdienste

Sind die richtigen Schutzdienste vorhanden? Bieten sie das richtige Maß an Abdeckung?

Schutzdienste helfen Ihnen, Angriffe und Gefährdungen abzuwehren, die auf den Service abzielen. Beispiele für Schutzdienste AWS sindAWS Control Tower,,AWS WAF, VantaAWS Shield Advanced, Secrets Manager, IAM Access Analyzer und. AWS Resource Access Manager

Sichere Entwicklung

Verwenden Sie sichere Codierungspraktiken?

Vermeiden Sie Schwachstellen wie das Open Web Application Security Project (OWASP) Top Ten?

Detect

Entwickeln und implementieren Sie geeignete Aktivitäten, um das Auftreten eines Cybersicherheitsereignisses zu identifizieren.

Erkennungsservices

Sind die richtigen Erkennungsservices vorhanden?

Bieten sie das richtige Maß an Abdeckung?

Beispiele für AWS Erkennungsdienste sind Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, Amazon Detective, Amazon CloudWatch Alarms undAWS IoT Device Defender. AWS Trusted Advisor

Reagieren

Entwickeln und implementieren Sie geeignete Aktivitäten, um Maßnahmen in Bezug auf ein erkanntes Cybersicherheitsereignis zu ergreifen.

Maßnahmen zur Reaktion

Reagieren Sie schnell auf Sicherheitsereignisse?

Verfügen Sie über aktive Ergebnisse mit kritischem oder hohem Schweregrad?

Forensik

Können Sie sicher forensische Daten für den Service erfassen? Erwerben Sie beispielsweise Amazon EBS-Snapshots, die mit wirklich positiven Ergebnissen verknüpft sind?

Haben Sie ein forensisches Konto eingerichtet?

Wiederherstellung

Entwickeln und implementieren Sie geeignete Aktivitäten, um Ausfallpläne aufrechtzuerhalten und alle Funktionen oder Services wiederherzustellen, die aufgrund eines Cybersicherheitsereignisses beeinträchtigt wurden.

Ausfallsicherheit

Unterstützt die Servicekonfiguration ordnungsgemäße Failovers, elastische Skalierung und hohe Verfügbarkeit?

Haben Sie Sicherungen erstellt?

Überprüfung der Details der Kontrollen in Security Hub CSPM

Wenn Sie auf der Seite „Kontrollen“ oder auf der Seite mit den Standarddetails der Security Hub CSPM-Konsole ein Steuerelement auswählen, gelangen Sie zu einer Seite mit Kontrolldetails.

Im oberen Bereich der Seite mit den Kontrolldetails wird der Kontrollstatus angezeigt. Der Kontrollstatus fasst die Leistung einer Kontrolle auf der Grundlage des Konformitätsstatus der Kontrollergebnisse zusammen. Security Hub CSPM generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Status sind nur für Steuerelemente verfügbar, die aktiviert werden, wenn Sie diese Seiten besuchen.

Auf der Seite mit den Kontrolldetails finden Sie auch eine Aufschlüsselung des Konformitätsstatus der Kontrollergebnisse der letzten 24 Stunden. Weitere Informationen zum Kontrollstatus und zum Konformitätsstatus finden Sie unterBewertung des Konformitätsstatus und des Kontrollstatus.

AWS Config Die Ressourcenaufzeichnung muss konfiguriert sein, damit der Kontrollstatus angezeigt wird. Nachdem der Kontrollstatus zum ersten Mal generiert wurde, aktualisiert Security Hub CSPM den Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse der letzten 24 Stunden.

Für Administratorkonten wird ein aggregierter Kontrollstatus für das Administratorkonto und die Mitgliedskonten angezeigt. Wenn Sie eine Aggregationsregion festgelegt haben, umfasst der Kontrollstatus die Ergebnisse aller verknüpften Regionen. Weitere Informationen zum Kontrollstatus finden Sie unterthe section called “Konformitätsstatus und Kontrollstatus”.

Sie können das Steuerelement auch auf der Seite mit den Kontrolldetails aktivieren oder deaktivieren.

> **Note**
>
> Nach der Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis der Status einer Erstkontrolle in den Regionen China und generiert wird. AWS GovCloud (US) Regions

Auf der Registerkarte „Standards und Anforderungen“ sind die Standards aufgeführt, für die eine Kontrolle aktiviert werden kann, sowie die Anforderungen an die Kontrolle aus verschiedenen Compliance-Frameworks.

Auf der Registerkarte „Prüfungen“ sind die aktiven Ergebnisse der Kontrolle der letzten 24 Stunden aufgeführt. Kontrollergebnisse werden generiert und aktualisiert, wenn Security Hub CSPM Sicherheitsprüfungen für die Kontrolle durchführt. Die Liste auf dieser Registerkarte enthält keine archivierten Ergebnisse.

Für jedes Ergebnis bietet die Liste Zugriff auf Ergebnisdetails wie den Konformitätsstatus und die zugehörige Ressource. Sie können auch den Workflow-Status jedes Ergebnisses festlegen und die Ergebnisse an benutzerdefinierte Aktionen senden. Weitere Informationen finden Sie unter Überprüfung und Verwaltung der Kontrollergebnisse.

Details für ein Steuerelement anzeigen

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie diesen Schritten, um die Details für ein Steuerelement zu überprüfen. Die Angaben beziehen sich auf das Girokonto und die Region und beinhalten Folgendes:

- Der Titel und die Beschreibung des Steuerelements.
- Ein Link zu Anleitungen zur Behebung fehlgeschlagener Kontrollversuche.
- Der Schweregrad der Kontrolle.
- Der Status der Kontrolle.

Auf der Konsole können Sie auch eine Liste der neuesten Ergebnisse für das Steuerelement überprüfen. Um dies programmgesteuert zu tun, können Sie den GetFindings Betrieb der Security Hub CSPM-API verwenden.

Security Hub CSPM console

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Steuerelemente aus.
3. Wählen Sie ein Steuerelement aus.

Security Hub CSPM API

1. Führen Sie `ListSecurityControlDefinitions` den Befehl aus und geben Sie eine oder mehrere Standard-ARNs ein, um eine Liste der Kontroll-IDs für diesen Standard abzurufen. Um Standard-ARNs abzurufen, führen Sie den Befehl aus. `DescribeStandards` Wenn Sie keinen Standard-ARN angeben, gibt diese API alle Security Hub CSPM-Steuerungs-IDs zurück. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, nicht die standardbasierten Kontroll-IDs, die vor diesen Feature-Releases existierten.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Ausführen`BatchGetSecurityControls`, um Details zu einem oder mehreren Steuerelementen im aktuellen AWS-Konto und abzurufen AWS-Region.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Führen Sie den `list-security-control-definitions` Befehl aus und geben Sie eine oder mehrere Standard-ARNs an, um eine Liste von Kontroll-IDs abzurufen. Führen Sie den Befehl aus, um Standard-ARNs abzurufen. `describe-standards` Wenn Sie keinen Standard-ARN angeben, gibt dieser Befehl alle Security Hub CSPM-Steuerungs-IDs zurück. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, nicht die standardbasierten Kontroll-IDs, die vor diesen Feature-Releases existierten.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
   ```

2. Führen Sie den `batch-get-security-controls` Befehl aus, um Details zu einem oder mehreren Steuerelementen im aktuellen und abzurufen. AWS-Konto AWS-Region

```
aws securityhub --region us-east-1 batch-get-security-controls --security-control-ids '["Config.1", "IAM.1"]'
```

Filter- und Sortierkontrollen in Security Hub CSPM

Auf der AWS Security Hub CSPM-Konsole können Sie auf der Seite „Kontrollen“ eine Tabelle der Steuerelemente einsehen, die in der aktuellen Version verfügbar sind. AWS-Region Die Ausnahme ist eine Aggregationsregion. Wenn Sie eine Aggregationsregion konfiguriert haben und sich bei dieser Region anmelden, zeigt die Konsole Steuerelemente an, die in der Aggregationsregion oder in einer oder mehreren verknüpften Regionen verfügbar sind.

Um sich auf eine bestimmte Untergruppe von Steuerelementen zu konzentrieren, können Sie die Kontrolltabelle sortieren und filtern. Mit den Optionen „Nach filtern“ neben der Tabelle können Sie sich schnell auf diese bestimmten Teilmengen konzentrieren:

- Alle aktivierten Steuerelemente, d. h. Steuerelemente, die in mindestens einem aktivierten Standard aktiviert sind.
- Alle deaktivierten Steuerelemente, d. h. Steuerelemente, die in allen Standards deaktiviert sind.
- Alle aktivierten Steuerelemente, die einen bestimmten Kontrollstatus haben, z. B. Fehlgeschlagen. Mit der Option Keine Daten werden nur die Steuerelemente angezeigt, für die derzeit keine Ergebnisse vorliegen. Informationen zum Kontrollstatus finden Sie unterBewertung des Konformitätsstatus und des Kontrollstatus.

Zusätzlich zu den Optionen Filtern nach können Sie die Tabelle filtern, indem Sie Filterkriterien in das Feld Filtersteuerelemente über der Tabelle eingeben. Sie können beispielsweise nach Kontroll-ID oder Schweregrad filtern.

Standardmäßig werden Steuerelemente mit dem Status Fehlgeschlagen an erster Stelle aufgeführt, und zwar in absteigender Reihenfolge nach Schweregrad. Sie können die Sortierreihenfolge ändern, indem Sie eine andere Spaltenüberschrift auswählen.

> **Tip**
>
> Wenn Sie automatisierte Workflows haben, die auf Kontrollergebnissen basieren, empfehlen wir, die Felder `SecurityControlId` oder `SecurityControlArn` ASFF als Filter zu verwenden und nicht die `Description` Felder `Title` oder. Die letztgenannten Felder können sich gelegentlich ändern, wohingegen Kontroll-ID und ARN statische Identifikatoren sind.

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, gehören zu den aktivierten Steuerelementen auch Steuerelemente, die in mindestens einem Mitgliedskonto aktiviert sind. Wenn Sie eine Aggregationsregion konfiguriert haben, umfassen die aktivierten Steuerelemente Steuerelemente, die in mindestens einer verknüpften Region aktiviert sind.

Wenn Sie die Option neben einem aktivierten Steuerelement auswählen, wird ein Fenster mit den Standards angezeigt, in denen das Steuerelement derzeit aktiviert ist. Sie können auch die Standards sehen, in denen das Steuerelement derzeit deaktiviert ist. In diesem Bereich können Sie ein Steuerelement in allen Standards deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Steuerelemente in Security Hub CSPM. Bei Administratorkonten entsprechen die Informationen im Panel den Einstellungen für alle Ihre Mitgliedskonten.

Um eine Liste von Steuerelementen programmgesteuert abzurufen, können Sie die ListSecurityControlDefinitions Security Hub CSPM-API verwenden. Verwenden Sie den Vorgang, um die Details einzelner Steuerelemente abzurufen. BatchGetSecurityControls

Grundlegendes zu den Steuerungsparametern in Security Hub CSPM

Einige Steuerelemente in AWS Security Hub CSPM verwenden Parameter, die beeinflussen, wie das Steuerelement ausgewertet wird. In der Regel werden solche Steuerelemente anhand der von Security Hub CSPM definierten Standardparameterwerte bewertet. Für eine Teilmenge dieser Steuerelemente können Sie die Parameterwerte jedoch ändern. Wenn Sie einen Steuerungsparameterwert ändern, beginnt Security Hub CSPM, das Steuerelement anhand des von Ihnen angegebenen Werts auszuwerten. Wenn die dem Steuerelement zugrunde liegende Ressource den benutzerdefinierten Wert erfüllt, generiert Security Hub CSPM ein Ergebnis. `PASSED` Wenn die Ressource den benutzerdefinierten Wert nicht erfüllt, generiert Security Hub CSPM ein Ergebnis. `FAILED`

Durch die Anpassung der Steuerungsparameter können Sie die von Security Hub CSPM empfohlenen und überwachten bewährten Sicherheitsmethoden verfeinern, um sie an Ihre

Geschäftsanforderungen und Sicherheitserwartungen anzupassen. Anstatt die Ergebnisse einer Kontrolle zu unterdrücken, können Sie einen oder mehrere ihrer Parameter anpassen, um Ergebnisse zu erhalten, die Ihren Sicherheitsanforderungen entsprechen.

Im Folgenden finden Sie einige Anwendungsbeispiele für das Ändern von Steuerungsparametern und das Festlegen benutzerdefinierter Werte:

- [CloudWatch.16] — CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

  Sie können den Aufbewahrungszeitraum angeben.
- [IAM.7] — Die Passwortrichtlinien für IAM-Benutzer sollten über starke Konfigurationen verfügen

  Sie können Parameter angeben, die sich auf die Passwortstärke beziehen.
- [EC2.18] — Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

  Sie können angeben, welche Ports uneingeschränkten eingehenden Datenverkehr zulassen dürfen.
- [Lambda.5] — VPC-Lambda-Funktionen sollten in mehreren Availability Zones ausgeführt werden

  Sie können die Mindestanzahl an Availability Zones angeben, die zu einem bestandenen Ergebnis führt.

In diesem Abschnitt werden Aspekte behandelt, die bei der Änderung von Steuerungsparametern zu berücksichtigen sind.

Auswirkung der Änderung von Steuerparameterwerten

Wenn Sie einen Parameterwert ändern, lösen Sie auch eine neue Sicherheitsüberprüfung aus, bei der das Steuerelement anhand des neuen Werts bewertet wird. Security Hub CSPM generiert dann neue Kontrollergebnisse auf der Grundlage des neuen Werts. Bei regelmäßigen Aktualisierungen der Kontrollergebnisse verwendet Security Hub CSPM ebenfalls den neuen Parameterwert. Wenn Sie die Parameterwerte für ein Steuerelement ändern, aber keine Standards aktiviert haben, die das Steuerelement enthalten, führt Security Hub CSPM keine Sicherheitsprüfungen mit den neuen Werten durch. Sie müssen mindestens einen relevanten Standard für Security Hub CSPM aktivieren, um die Steuerung anhand des neuen Parameterwerts bewerten zu können.

Ein Steuerelement kann einen oder mehrere anpassbare Parameter haben. Zu den möglichen Datentypen für jeden Steuerungsparameter gehören die folgenden:

- Boolesch
- Double
- Enum
- EnumList
- Ganzzahl
- IntegerList
- Zeichenfolge
- StringList

Benutzerdefinierte Parameterwerte gelten für alle aktivierten Standards. Sie können die Parameter für ein Steuerelement, das in Ihrer aktuellen Region nicht unterstützt wird, nicht anpassen. Eine Liste der regionalen Grenzwerte für einzelne Steuerelemente finden Sie unterRegionale Beschränkungen der Security Hub CSPM-Steuerungen.

Bei einigen Steuerelementen müssen akzeptable Parameterwerte in einen bestimmten Bereich fallen, um gültig zu sein. In diesen Fällen bietet Security Hub CSPM den akzeptablen Bereich.

Security Hub CSPM wählt Standardparameterwerte aus und aktualisiert sie möglicherweise gelegentlich. Nachdem Sie einen Steuerparameter angepasst haben, ist sein Wert weiterhin der Wert, den Sie für den Parameter angegeben haben, sofern Sie ihn nicht ändern. Das heißt, der Parameter stoppt die Verfolgung von Aktualisierungen des Security Hub CSPM-Standardwerts, auch wenn der benutzerdefinierte Wert des Parameters mit dem aktuellen, von Security Hub CSPM definierten Standardwert übereinstimmt. Hier ist ein Beispiel für die Steuerung [ACM.1] — Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
```

```
    }
}
```

Im vorherigen Beispiel hat der `daysToExpiration` Parameter einen benutzerdefinierten Wert von`30`. Der aktuelle Standardwert für diesen Parameter ist ebenfalls`30`. Wenn Security Hub CSPM den Standardwert auf ändert`14`, verfolgt der Parameter in diesem Beispiel diese Änderung nicht. Er behält einen Wert von bei. `30`

Wenn Sie Aktualisierungen des Security Hub CSPM-Standardwerts für einen Parameter nachverfolgen möchten, setzen Sie das `ValueType` Feld auf `DEFAULT` statt. `CUSTOM` Weitere Informationen finden Sie unter Zurücksetzen auf die Standardsteuerungsparameter in einem einzelnen Konto und einer Region.

Steuerelemente, die benutzerdefinierte Parameter unterstützen

Eine Liste der Sicherheitskontrollen, die benutzerdefinierte Parameter unterstützen, finden Sie auf der Seite Steuerelemente der Security Hub CSPM-Konsole oder im. Kontrollreferenz für Security Hub CSPM Um diese Liste programmgesteuert abzurufen, können Sie den Vorgang verwenden. ListSecurityControlDefinitions In der Antwort gibt das `CustomizableProperties` Objekt an, welche Steuerelemente anpassbare Parameter unterstützen.

Aktuelle Steuerungsparameterwerte werden überprüft

Es kann hilfreich sein, den aktuellen Wert eines Steuerparameters zu kennen, bevor Sie ihn ändern.

Sie können die aktuellen Werte für einzelne Steuerparameter in Ihrem Konto überprüfen. Wenn Sie die zentrale Konfiguration verwenden, kann der beauftragte AWS Security Hub CSPM-Administrator auch die in einer Konfigurationsrichtlinie angegebenen Parameterwerte überprüfen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die aktuellen Steuerungsparameterwerte zu überprüfen.

Security Hub CSPM console

Um die aktuellen Werte der Steuerungsparameter zu überprüfen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie ein Steuerelement aus.

3. Wählen Sie die Registerkarte Parameters aus. Auf dieser Registerkarte werden die aktuellen Parameterwerte für das Steuerelement angezeigt.

Security Hub CSPM API

Um die aktuellen Steuerungsparameterwerte zu überprüfen (API)

Rufen Sie die BatchGetSecurityControls API auf und geben Sie eine oder mehrere Sicherheitskontroll-IDs oder ARNs an. Das `Parameters` Objekt in der Antwort zeigt die aktuellen Parameterwerte für die angegebenen Steuerelemente.

Der folgende AWS CLI Befehl zeigt beispielsweise die aktuellen Parameterwerte für `APIGatway.1` `CloudWatch.15`, und`IAM.7`. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Wählen Sie Ihre bevorzugte Methode, um die aktuellen Parameterwerte in einer zentralen Konfigurationsrichtlinie anzuzeigen.

Security Hub CSPM console

Um die aktuellen Steuerungsparameterwerte in einer Konfigurationsrichtlinie (Konsole) zu überprüfen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Richtlinien die Konfigurationsrichtlinie aus, und klicken Sie dann auf Details anzeigen. Die Richtliniendetails werden dann angezeigt, einschließlich der aktuellen Parameterwerte.

Security Hub CSPM API

Um die aktuellen Steuerungsparameterwerte in einer Konfigurationsrichtlinie (API) zu überprüfen

1. Rufen Sie die GetConfigurationPolicy API über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie den ARN oder die ID der Konfigurationsrichtlinie an, deren Details Sie sehen möchten. Die Antwort enthält aktuelle Parameterwerte.

Mit dem folgenden AWS CLI Befehl werden beispielsweise die aktuellen Steuerungsparameterwerte in der angegebenen Konfigurationsrichtlinie abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Zu den Kontrollergebnissen gehören auch die aktuellen Werte der Steuerungsparameter. In der AWS Format für Sicherheitssuche (ASFF) erscheinen diese Werte im `Parameters` Feld des `Compliance` Objekts. Um die Ergebnisse auf der Security Hub CSPM-Konsole zu überprüfen, wählen Sie im Navigationsbereich Ergebnisse aus. Um die Ergebnisse programmatisch zu überprüfen, verwenden Sie den GetFindings Betrieb der Security Hub CSPM-API.

Anpassen der Steuerungsparameterwerte

Die Anweisungen zum Anpassen der Steuerungsparameter variieren je nachdem, ob Sie die zentrale Konfiguration in AWS Security Hub CSPM verwenden. Die zentrale Konfiguration ist eine Funktion, die der delegierte Security Hub CSPM-Administrator verwenden kann, um die Security Hub CSPM-Funktionen für Konten und Organisationseinheiten (OUs) AWS-Regionen zu konfigurieren.

Wenn Ihre Organisation die zentrale Konfiguration verwendet, kann der delegierte Administrator Konfigurationsrichtlinien erstellen, die benutzerdefinierte Steuerparameter enthalten. Diese Richtlinien können zentral verwalteten Mitgliedskonten und Organisationseinheiten zugeordnet werden und treten in Ihrer Heimatregion und allen verknüpften Regionen in Kraft. Der delegierte Administrator

kann auch ein oder mehrere Konten als selbstverwaltete Konten festlegen, sodass der Kontoinhaber seine eigenen Parameter in jeder Region separat konfigurieren kann. Wenn Ihre Organisation keine zentrale Konfiguration verwendet, müssen Sie die Steuerungsparameter für jedes Konto und jede Region separat anpassen.

Wir empfehlen, die zentrale Konfiguration zu verwenden, da Sie damit die Werte der Steuerungsparameter in verschiedenen Teilen Ihrer Organisation aufeinander abstimmen können. Beispielsweise verwenden möglicherweise alle Ihre Testkonten bestimmte Parameterwerte, und alle Produktionskonten verwenden möglicherweise unterschiedliche Werte.

Anpassen der Steuerungsparameter in mehreren Konten und Regionen

Wenn Sie der delegierte Security Hub CSPM-Administrator für eine Organisation sind, die die zentrale Konfiguration verwendet, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Anpassung der Steuerungsparameter für mehrere Konten und Regionen.

Security Hub CSPM console

So passen Sie die Werte der Steuerungsparameter in mehreren Konten und Regionen an (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

   Stellen Sie sicher, dass Sie in der Heimatregion angemeldet sind.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Um eine neue Konfigurationsrichtlinie zu erstellen, die benutzerdefinierte Parameter enthält, wählen Sie Create policy aus. Um benutzerdefinierte Parameter in einer vorhandenen Konfigurationsrichtlinie anzugeben, wählen Sie die Richtlinie aus und klicken Sie dann auf Bearbeiten.

   Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Steuerparameterwerten zu erstellen

   1. Wählen Sie im Abschnitt Benutzerdefinierte Richtlinie die Sicherheitsstandards und Steuerelemente aus, die Sie aktivieren möchten.
   2. Wählen Sie Steuerungsparameter anpassen aus.

3. Wählen Sie ein Steuerelement aus, und geben Sie dann benutzerdefinierte Werte für einen oder mehrere Parameter an.
4. Um die Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.
5. Wählen Sie im Abschnitt Konten die Konten oder Organisationseinheiten aus, auf die Sie die Richtlinie anwenden möchten.
6. Wählen Sie Weiter aus.
7. Wählen Sie Richtlinie erstellen und anwenden aus. In Ihrer Heimatregion und allen verknüpften Regionen überschreibt diese Aktion die vorhandenen Konfigurationseinstellungen von Konten und Organisationseinheiten, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können einer Konfigurationsrichtlinie durch direkte Anwendung oder durch Vererbung von einem übergeordneten Objekt zugeordnet werden.

Um die Werte der Steuerungsparameter in einer vorhandenen Konfigurationsrichtlinie anzupassen

1. Geben Sie im Abschnitt Steuerelemente unter Benutzerdefinierte Richtlinie die gewünschten neuen benutzerdefinierten Parameterwerte an.
2. Wenn Sie die Steuerungsparameter in dieser Richtlinie zum ersten Mal anpassen, wählen Sie Steuerungsparameter anpassen aus, und wählen Sie dann ein Steuerelement aus, das Sie anpassen möchten. Um die Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.
3. Überprüfen Sie im Abschnitt Konten die Konten oder Organisationseinheiten, auf die Sie die Richtlinie anwenden möchten.
4. Wählen Sie Weiter aus.
5. Überprüfe deine Änderungen und vergewissere dich, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen überschreibt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten und Organisationseinheiten, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können einer Konfigurationsrichtlinie durch direkte Anwendung oder durch Vererbung von einem übergeordneten Objekt zugeordnet werden.

Security Hub CSPM API

Zur Anpassung der Steuerungsparameterwerte in mehreren Konten und Regionen (API)

Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Steuerparameterwerten zu erstellen

1. Rufen Sie die CreateConfigurationPolicy API über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `SecurityControlCustomParameters` Objekt den Bezeichner jedes Steuerelements an, das Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` ein`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Das `Value` Feld darf nicht leer sein, wenn `ValueType` es ist`CUSTOM`. Wenn Ihre Anfrage einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinition API aufrufen.

So passen Sie Steuerungsparameterwerte in einer vorhandenen Konfigurationsrichtlinie an

1. Rufen Sie die UpdateConfigurationPolicy API vom Konto des delegierten Administrators in der Heimatregion aus auf.
2. Geben Sie für das `Identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das `SecurityControlCustomParameters` Objekt die Kennung jedes Steuerelements an, das Sie anpassen möchten.
4. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` ein`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn Ihre Anforderung einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinition API aufrufen.

Mit dem folgenden AWS CLI Befehl wird beispielsweise eine neue Konfigurationsrichtlinie mit einem benutzerdefinierten Wert für den `daysToExpiration` Parameter von `ACM.1` erstellt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Anpassen der Steuerparameter in einem einzelnen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie die Steuerungsparameter für Ihr Konto jeweils nur in einer Region anpassen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Anpassung der Steuerungsparameter. Ihre Änderungen gelten nur für Ihr Konto in der aktuellen Region. Um die Steuerungsparameter in weiteren Regionen anzupassen, wiederholen Sie die folgenden Schritte für jedes weitere Konto und jede Region, in der Sie Parameter anpassen möchten. Dieselbe Steuerung kann unterschiedliche Parameterwerte in verschiedenen Regionen verwenden.

Security Hub CSPM console

Um die Werte der Steuerungsparameter in einem Konto und einer Region (Konsole) anzupassen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie in der Tabelle ein Steuerelement aus, das benutzerdefinierte Parameter unterstützt und für das Sie die Parameter ändern möchten. In der Spalte Benutzerdefinierte Parameter wird angegeben, welche Steuerelemente benutzerdefinierte Parameter unterstützen.

3. Wählen Sie auf der Detailseite für das Steuerelement die Registerkarte Parameter aus, und klicken Sie dann auf Bearbeiten.
4. Geben Sie die gewünschten Parameterwerte an.
5. Wählen Sie optional im Abschnitt Grund für die Änderung einen Grund für die Anpassung der Parameter aus.
6. Wählen Sie Speichern.

Security Hub CSPM API

Um die Werte der Steuerungsparameter in einem Konto und einer Region (API) anzupassen

1. Rufen Sie die UpdateSecurityControl API auf.
2. Geben Sie `SecurityControlId` beispielsweise die ID des Steuerelements an, das Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` ein`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn Ihre Anforderung einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinition API aufrufen.
4. Geben Sie optional einen Grund für `LastUpdateReason` die Anpassung der Steuerungsparameter an.

Beispielsweise definiert der folgende AWS CLI Befehl einen benutzerdefinierten Wert für den `daysToExpiration` Parameter von`ACM.1`. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Zu den Standardwerten der Steuerparameter zurückkehren

Ein Steuerungsparameter kann einen Standardwert haben, den AWS Security Hub CSPM definiert. Gelegentlich aktualisiert Security Hub CSPM den Standardwert für einen Parameter, um den sich ändernden bewährten Sicherheitsmethoden Rechnung zu tragen. Wenn Sie keinen benutzerdefinierten Wert für einen Steuerungsparameter angegeben haben, verfolgt das Steuerelement diese Aktualisierungen automatisch und verwendet den neuen Standardwert.

Sie können wieder Standardparameterwerte für ein Steuerelement verwenden. Die Anweisungen für die Umkehrung hängen davon ab, ob Sie die zentrale Konfiguration in Security Hub CSPM verwenden. Die zentrale Konfiguration ist eine Funktion, die der delegierte Security Hub CSPM-Administrator verwenden kann, um die Security Hub CSPM-Funktionen für Konten und Organisationseinheiten (OUs) AWS-Regionen zu konfigurieren.

> **Note**
>
> Nicht alle Steuerungsparameter haben einen Standardwert für Security Hub CSPM. In solchen Fällen, wenn auf gesetzt `ValueType` ist`DEFAULT`, gibt es keinen bestimmten Standardwert, den Security Hub CSPM verwendet. Vielmehr ignoriert Security Hub CSPM den Parameter, wenn kein benutzerdefinierter Wert vorhanden ist.

Rückkehr zu den Standardsteuerungsparametern in mehreren Konten und Regionen

Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerungsparameter für mehrere zentral verwaltete Konten und Organisationseinheiten in der Heimatregion und verknüpften Regionen zurücksetzen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um mithilfe der zentralen Konfiguration die Standardparameterwerte für mehrere Konten und Regionen wiederherzustellen.

Security Hub CSPM console

So kehren Sie in mehreren Konten und Regionen zu den Standardwerten der Steuerungsparameter zurück (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie eine Richtlinie aus und klicken Sie dann auf Bearbeiten.
5. Unter Benutzerdefinierte Richtlinie wird im Abschnitt Steuerelemente eine Liste der Steuerelemente angezeigt, für die Sie benutzerdefinierte Parameter angegeben haben.
6. Suchen Sie das Steuerelement, das über einen oder mehrere Parameterwerte verfügt, die rückgängig gemacht werden sollen. Wählen Sie dann Entfernen, um zu den Standardwerten zurückzukehren.
7. Überprüfen Sie im Abschnitt Konten die Konten oder Organisationseinheiten, auf die Sie die Richtlinie anwenden möchten.
8. Wählen Sie Weiter aus.
9. Überprüfe deine Änderungen und vergewissere dich, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen überschreibt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten und Organisationseinheiten, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können einer Konfigurationsrichtlinie durch direkte Anwendung oder durch Vererbung von einem übergeordneten Objekt zugeordnet werden.

Security Hub CSPM API

Um in mehreren Konten und Regionen (API) zu den Standardwerten der Steuerungsparameter zurückzukehren

1. Rufen Sie die UpdateConfigurationPolicy API vom Konto des delegierten Administrators in der Heimatregion aus auf.
2. Geben Sie für das `Identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Richtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das `SecurityControlCustomParameters` Objekt den Bezeichner jedes Steuerelements an, für das Sie einen oder mehrere Parameter rückgängig machen möchten.
4. Geben Sie im `Parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`,

müssen Sie keinen Wert für das `Value` Feld angeben. Wenn Ihre Anfrage einen Wert enthält, ignoriert Security Hub CSPM ihn. Wenn Ihre Anfrage einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei.

> **Warning**
>
> Wenn Sie ein Steuerobjekt aus dem `SecurityControlCustomParameters` Feld weglassen, setzt Security Hub CSPM alle benutzerdefinierten Parameter für das Steuerelement auf ihre Standardwerte zurück. Eine vollständig leere Liste für `SecurityControlCustomParameters` setzt benutzerdefinierte Parameter für alle Steuerelemente auf ihre Standardwerte zurück.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der `daysToExpiration` Steuerparameter für `ACM.1` auf den Standardwert in der angegebenen Konfigurationsrichtlinie zurückgesetzt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Zurücksetzen auf die Standardsteuerungsparameter in einem einzelnen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie die Standardparameterwerte für Ihr Konto in einer Region nach der anderen verwenden.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Standardparameterwerte für Ihr Konto in einer einzelnen Region wiederherzustellen. Um in weiteren Regionen zu den Standardparameterwerten zurückzukehren, wiederholen Sie diese Schritte in jeder weiteren Region.

> **Note**
>
> Wenn Sie Security Hub CSPM deaktivieren, werden Ihre benutzerdefinierten Steuerungsparameter zurückgesetzt. Wenn Sie Security Hub CSPM in Zukunft erneut aktivieren, verwenden alle Steuerelemente beim Start die Standardparameterwerte.

Security Hub CSPM console

So kehren Sie zu den Standardwerten der Steuerungsparameter in einem Konto und einer Region (Konsole) zurück

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie das Steuerelement aus, das Sie auf die Standardparameterwerte zurücksetzen möchten.
3. Wählen Sie auf der **`Parameters`** Registerkarte neben einem Steuerparameter die Option Benutzerdefiniert aus. Wählen Sie dann Anpassung entfernen aus. Dieser Parameter verwendet jetzt den CSPM-Standardwert von Security Hub und verfolgt zukünftige Aktualisierungen auf den Standardwert.
4. Wiederholen Sie den vorherigen Schritt für jeden Parameterwert, den Sie zurücksetzen möchten.

Security Hub CSPM API

So kehren Sie zu den Standardwerten der Steuerungsparameter in einem Konto und einer Region (API) zurück

1. Rufen Sie die API auf UpdateSecurityControl.
2. Geben Sie `SecurityControlId` beispielsweise den ARN oder die ID des Steuerelements an, dessen Parameter Sie rückgängig machen möchten.
3. Geben Sie im `Parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`,

müssen Sie keinen Wert für das `Value` Feld angeben. Wenn Ihre Anfrage einen Wert enthält, ignoriert Security Hub CSPM ihn.

4. Geben Sie optional einen Grund für `LastUpdateReason` die Rückkehr zu den Standardparameterwerten an.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der `daysToExpiration` Steuerparameter für `ACM.1` auf seinen Standardwert zurückgesetzt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Überprüfung des Status der Änderungen der Steuerparameter

Wenn Sie versuchen, einen Steuerparameter anzupassen oder zum Standardwert zurückzukehren, können Sie überprüfen, ob die gewünschten Änderungen wirksam waren. Auf diese Weise können Sie sicherstellen, dass ein Steuerelement erwartungsgemäß funktioniert und den beabsichtigten Sicherheitswert bietet. Wenn eine Parameteraktualisierung nicht erfolgreich ist, behält Security Hub CSPM den aktuellen Wert für den Parameter bei.

Um zu überprüfen, ob ein Parameterupdate erfolgreich war, können Sie die Details der Steuerung auf der Security Hub CSPM-Konsole überprüfen. Wählen Sie auf der Konsole im Navigationsbereich Controls aus. Wählen Sie dann ein Steuerelement aus, um dessen Details anzuzeigen. Auf der Registerkarte Parameter wird der Status der Parameteränderung angezeigt.

Wenn Ihre Anforderung zum Aktualisieren eines Parameters gültig ist, ist der Wert des `UpdateStatus` Felds programmatisch eine Antwort auf den BatchGetSecurityControls Vorgang. `UPDATING` Das bedeutet, dass die Aktualisierung gültig war, aber möglicherweise noch nicht alle Ergebnisse die aktualisierten Parameterwerte enthalten. Wenn sich der Wert von auf `UpdateState` ändert`READY`, verwendet Security Hub CSPM die aktualisierten Steuerungsparameterwerte, wenn Sicherheitsüberprüfungen des Steuerelements ausgeführt werden. Die Ergebnisse beinhalten die aktualisierten Parameterwerte.

Der `UpdateSecurityControl` Vorgang gibt eine `InvalidInputException` Antwort für ungültige Parameterwerte zurück. Die Antwort enthält zusätzliche Details zum Grund des Fehlers. Beispielsweise haben Sie möglicherweise einen Wert angegeben, der außerhalb des gültigen Bereichs für einen Parameter liegt. Oder Sie haben möglicherweise einen Wert angegeben, der nicht den richtigen Datentyp verwendet. Senden Sie Ihre Anfrage erneut mit einer gültigen Eingabe.

Wenn beim Versuch, einen Parameterwert zu aktualisieren, ein interner Fehler auftritt, versucht Security Hub CSPM automatisch erneut, sofern Sie ihn aktiviert haben. AWS Config Weitere Informationen finden Sie unter Überlegungen vor der Aktivierung und Konfiguration AWS Config.

Überprüfung und Verwaltung der Kontrollergebnisse in Security Hub CSPM

Auf der Seite mit den Kontrolldetails wird eine Liste der aktiven Ergebnisse für eine Kontrolle angezeigt. Die Liste enthält keine archivierten Ergebnisse.

Die Seite mit den Kontrolldetails unterstützt die regionsübergreifende Aggregation. Wenn Sie eine Aggregationsregion festgelegt haben, enthalten der Kontrollstatus und die Liste der Sicherheitsüberprüfungen auf der Seite mit den Kontrolldetails die Prüfungen aller verknüpften Kontrollen. AWS-Regionen

Die Liste enthält Tools zum Filtern und Sortieren der Ergebnisse, sodass Sie sich zuerst auf dringendere Ergebnisse konzentrieren können. Ein Ergebnis kann Links zu Ressourcendetails in der entsprechenden Servicekonsole enthalten. Bei Steuerelementen, die auf AWS Config Regeln basieren, können Sie sich Details zu der Regel anzeigen lassen.

Sie können auch die AWS Security Hub CSPM-API verwenden, um eine Liste mit Ergebnissen und Ergebnisdetails abzurufen.

Weitere Informationen finden Sie unter Details und Verlauf der Ergebnisse überprüfen.

Um den aktuellen Status Ihrer Untersuchung eines Kontrollbefundes widerzuspiegeln, legen Sie den Workflow-Status fest. Weitere Informationen finden Sie unter the section called “Den Workflow-Status von Ergebnissen festlegen”.

Sie können auch ausgewählte Security Hub CSPM-Ergebnisse an eine benutzerdefinierte Aktion in Amazon senden. EventBridge Weitere Informationen finden Sie unter the section called “Senden von Ergebnissen an eine benutzerdefinierte Aktion”.

Themen

- Filterung und Sortierung der Kontrollergebnisse

- Stichproben von Kontrollbefunden

Filterung und Sortierung der Kontrollergebnisse

Wenn Sie ein Steuerelement auf der Kontrollseite der AWS Security Hub CSPM-Konsole oder auf der Detailseite eines Standards auswählen, gelangen Sie zur Seite mit den Kontrolldetails.

Auf der Seite mit den Kontrolldetails werden der Titel und die Beschreibung der Kontrolle, der allgemeine Kontrollstatus und eine Aufschlüsselung der Sicherheitsüberprüfungen für die Kontrolle in den letzten 24 Stunden angezeigt.

Verwenden Sie die Option „Nach filtern“ neben der Liste der Kontrollprüfungen, um sich schnell auf Ergebnisse mit einem bestimmten Workflow - oder Compliance-Status zu konzentrieren.

Zusätzlich zu den Optionen Filtern nach können Sie das Feld Filter hinzufügen verwenden, um die Prüfliste nach anderen Feldern wie AWS-Konto ID oder Ressourcen-ID zu filtern.

Standardmäßig werden Ergebnisse mit dem Konformitätsstatus BESTANDEN zuerst aufgeführt. Sie können die Standardsortierung ändern, indem Sie in den Spaltenüberschriften eine andere Option auswählen.

Auf der Seite mit den Kontrolldetails können Sie Herunterladen wählen, um die aktuelle Seite mit den Kontrollergebnissen in eine CSV-Datei herunterzuladen.

Wenn Sie die Ergebnisliste filtern, umfasst der Download nur die Steuerelemente, die dem Filter entsprechen. Wenn Sie bestimmte Ergebnisse aus der Liste auswählen, enthält der Download nur die ausgewählten Ergebnisse.

Weitere Informationen zum Filtern von Ergebnissen finden Sie unterErgebnisse im Security Hub CSPM filtern.

Stichproben von Kontrollbefunden

Die folgenden Beispiele enthalten Beispiele für Ergebnisse der AWS Security Hub CSPM-Steuerung im AWS Security Finding Format (ASFF). Der Inhalt der Kontrollergebnisse hängt davon ab, ob Sie konsolidierte Kontrollergebnisse aktiviert haben.

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub CSPM ein einzelnes Ergebnis für eine Kontrolle, auch wenn die Kontrolle für mehrere aktivierte Standards gilt. Wenn Sie diese Funktion nicht aktivieren, generiert Security Hub CSPM für jeden aktivierten Standard, für den ein Steuerelement gilt, einen separaten Kontrollbefund. Wenn Sie beispielsweise zwei Standards

aktivieren und eine Kontrolle für beide gilt, erhalten Sie zwei separate Ergebnisse für die Kontrolle, einen für jeden Standard. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis für die Kontrolle. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Die Beispiele auf dieser Seite enthalten Beispiele für beide Szenarien. Zu den Stichproben gehören: Kontrollergebnisse für einzelne Security Hub CSPM-Standards, wenn konsolidierte Kontrollergebnisse deaktiviert sind, und Kontrollbefunde für mehrere Security Hub CSPM-Standards, wenn konsolidierte Kontrollergebnisse aktiviert sind.

Stichproben von Kontrollbefunden

- Stichprobenermittlung fürAWSStandard für grundlegende bewährte Sicherheitsverfahren
- Probenfindung für CISAWSBenchmark für Grundlagen v5.0.0
- Probenfindung für CISAWSBenchmark für Grundlagen v3.0.0
- Probenfindung für CISAWSBenchmark v1.4.0 für Stiftungen
- Probenfindung für CISAWSBenchmark v1.2.0 für Stiftungen
- Stichprobenergebnis für den Standard NIST SP 800-53 Revision 5
- Stichprobenergebnis für den Standard NIST SP 800-171 Revision 2
- Ergebnis eines Beispiels für den Datensicherheitsstandard v3.2.1 der Payment Card Industry
- Stichprobenergebnis fürAWSStandard für Ressourcen-Tagging
- Stichprobenergebnis fürAWS Control TowerStandard, der vom Service verwaltet wird
- Stichprobe: konsolidiertes Ergebnis für mehrere Standards

> **Note**
>
> Die Kontrollergebnisse beziehen sich auf verschiedene Felder und Werte in den Regionen China und den AWS GovCloud (US) Regionen. Weitere Informationen finden Sie unter Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte.

Stichprobenermittlung fürAWSStandard für grundlegende bewährte Sicherheitsverfahren

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den FSBP-Standard (AWSFoundational Security Best Practices) gilt. In diesem Beispiel ist die Option „Consolidated Control Findings“ deaktiviert.

```
{
```

```
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
```

```
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
```

```
  }
}
```

Probenfindung für CISAWSBenchmark für Grundlagen v5.0.0

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v5.0.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "AwsAccountId": "123456789012",
  "CompanyName": "AWS",
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.7",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v5.0.0/5.1.1"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/5.0.0"
      }
    ]
  },
  "CreatedAt": "2025-10-10T17:04:00.952Z",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Product": 40,
      "Original": "MEDIUM"
    }
  },
  "FirstObservedAt": "2025-10-10T17:03:57.895Z",
  "GeneratorId": "cis-aws-foundations-benchmark/v/5.0.0/5.1.1",
```

```
  "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
  "LastObservedAt": "2025-10-14T05:22:28.667Z",
  "ProcessedAt": "2025-10-14T05:22:50.099Z",
  "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/5.0.0",
    "ControlId": "5.1.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2a99554f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-west-1:123456789012:control/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-1::product/aws/
securityhub/arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
    "PreviousComplianceStatus": "FAILED"
  },
  "ProductName": "Security Hub CSPM",
  "RecordState": "ACTIVE",
  "Region": "us-west-1",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "Resources": [
    {
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-west-1",
      "Type": "AwsAccount"
    }
  ],
```

```
  "SchemaVersion": "2018-10-08",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM",
    "Product": 40
  },
  "Title": "5.1.1 EBS default encryption should be enabled",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "UpdatedAt": "2025-10-14T05:22:38.671Z",
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW"
}
```

Probenfindung für CISAWSBenchmark für Grundlagen v3.0.0

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v3.0.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
```

```
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
```

```
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Probenfindung für CISAWSBenchmark v1.4.0 für Stiftungen

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v1.4.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
```

```
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrailis a web service that recordsAWSAPI calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies.AWS Key Management Service(KMS) is a managed service that helps create and
 control the encryption keys used to encrypt account data, and uses Hardware Security
 Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be
 configured to leverage server side encryption (SSE) andAWS KMScustomer created master
 keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be
 configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
```

```
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CISAWSFoundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
```

```
  }
}
```

Probenfindung für CISAWSBenchmark v1.2.0 für Stiftungen

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v1.2.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service(KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
```

```
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Stichprobenergebnis für den Standard NIST SP 800-53 Revision 5

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für eine Kontrolle, die für den Standard NIST SP 800-53 Revision 5 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
```

```
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult theAWSSecurity Hub CSPM
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Stichprobenergebnis für den Standard NIST SP 800-171 Revision 2

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für eine Kontrolle, das für den Standard NIST SP 800-171 Revision 2 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
```

```
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
```

```
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
```

```
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Ergebnis eines Beispiels für den Datensicherheitsstandard v3.2.1 der Payment Card Industry

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest usingAWS
 KMSCMKs",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Stichprobenergebnis fürAWSStandard für Ressourcen-Tagging

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den AWS Resource Tagging-Standard gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
```

```
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
```

```
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
           },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Stichprobenergebnis fürAWS Control TowerStandard, der vom Service verwaltet wird

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den vom AWS Control Tower Service verwalteten Standard gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
```

```
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Stichprobe: konsolidiertes Ergebnis für mehrere Standards

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für mehrere aktivierte Standards gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse aktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
```

```
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
```

```
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```


Integrationen in Security Hub CSPM verstehen

AWS Security Hub CSPM kann Sicherheitsergebnisse von mehreren AWS-Services und unterstützten Sicherheitslösungen von Drittanbietern AWS Partner Network aufnehmen. Diese Integrationen können Ihnen helfen, sich einen umfassenden Überblick über Sicherheit und Compliance in Ihrer gesamten Umgebung zu verschaffen. AWS Security Hub CSPM nimmt Erkenntnisse aus integrierten Lösungen auf und konvertiert sie in das AWS Security Finding Format (ASFF).

Important

Bei unterstützten Produktintegrationen AWS und Integrationen von Drittanbietern empfängt und konsolidiert Security Hub CSPM die Ergebnisse, die erst generiert werden, nachdem Sie Security Hub CSPM für Ihren aktiviert haben. AWS-Konten Der Service empfängt und

konsolidiert nicht rückwirkend Sicherheitserkenntnisse, die vor der Aktivierung von Security Hub CSPM generiert wurden.

Die Seite Integrationen der Security Hub CSPM-Konsole bietet Zugriff auf verfügbare Produktintegrationen AWS und Produktintegrationen von Drittanbietern. Die Security Hub CSPM-API bietet auch Funktionen zur Verwaltung von Integrationen.

Eine Integration ist möglicherweise nicht in allen verfügbar. AWS-Regionen Wenn eine Integration in der Region, in der Sie derzeit angemeldet sind, auf der Security Hub CSPM-Konsole nicht unterstützt wird, wird sie nicht auf der Integrationsseite der Konsole angezeigt. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unterVerfügbarkeit von Integrationen nach Regionen.

Zusätzlich zu den AWS-Service integrierten Integrationen von Drittanbietern können Sie benutzerdefinierte Sicherheitsprodukte in Security Hub CSPM integrieren. Anschließend können Sie die Ergebnisse dieser Produkte mithilfe der Security Hub CSPM-API an Security Hub CSPM senden. Sie können die API auch verwenden, um bestehende Ergebnisse zu aktualisieren, die Security Hub CSPM von einem benutzerdefinierten Sicherheitsprodukt erhalten hat.

Themen

- Überprüfung einer Liste der Security Hub CSPM-Integrationen
- Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen
- Deaktivierung des Erkenntnisflusses aus einer Security Hub CSPM-Integration
- Ergebnisse einer Security Hub CSPM-Integration anzeigen
- AWS-Service Integrationen mit Security Hub CSPM
- Third-party Produktintegrationen mit Security Hub CSPM
- Integration von Security Hub CSPM mit kundenspezifischen Produkten

Überprüfung einer Liste der Security Hub CSPM-Integrationen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Liste der Integrationen in AWS Security Hub CSPM oder Details zu einer bestimmten Integration einzusehen.

Security Hub CSPM console

Um die Integrationsoptionen und Details zu überprüfen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.

Auf der Seite Integrationen AWS-Services werden Integrationen mit anderen zuerst aufgeführt, gefolgt von Integrationen mit Produkten von Drittanbietern.

Für jede Integration enthält die Seite Integrationen die folgenden Informationen:

- Der Name des Unternehmens
- Der Name des Produkts.
- Eine Beschreibung der Integration.
- Die Kategorien, für die die Integration gilt
- So aktivieren Sie die Integration:
- Der aktuelle Status der Integration

Sie können die Liste filtern, indem Sie Text aus den folgenden Feldern eingeben:

- Unternehmensname
- Product Name (Produktname)
- Beschreibung der Integration
- Kategorien

Security Hub CSPM API

Um die Integrationsoptionen und -details (API) zu überprüfen

Verwenden Sie den DescribeProductsVorgang, um eine Liste der Integrationen zu erhalten. Wenn Sie den verwenden AWS CLI, führen Sie den describe-productsBefehl aus.

Um Details für eine bestimmte Produktintegration abzurufen, verwenden Sie den `ProductArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Integration anzugeben.

Mit dem folgenden AWS CLI Befehl werden beispielsweise Details zur Security Hub CSPM-Integration mit 3CoreSec abgerufen.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen

Auf der Seite Integrationen der AWS Security Hub CSPM-Konsole sehen Sie die erforderlichen Schritte, um die einzelnen Integrationen zu aktivieren.

Bei den meisten Integrationen mit anderen AWS-Services ist der einzige erforderliche Schritt zur Aktivierung der Integration die Aktivierung des anderen Dienstes. Die Integrationsinformationen enthalten einen Link zur Homepage des anderen Dienstes. Wenn Sie den anderen Dienst aktivieren, wird automatisch eine Berechtigung auf Ressourcenebene erstellt und angewendet, die es Security Hub CSPM ermöglicht, Ergebnisse von dem Dienst zu empfangen.

Bei Produktintegrationen von Drittanbietern müssen Sie die Integration möglicherweise bei der erwerben und anschließend AWS Marketplace konfigurieren. Die Integrationsinformationen enthalten Links, mit denen Sie diese Aufgaben ausführen können.

Wenn mehrere Versionen eines Produkts verfügbar sind AWS Marketplace, wählen Sie die Version aus, die Sie abonnieren möchten, und klicken Sie dann auf Weiter abonnieren. Einige Produkte bieten beispielsweise eine Standardversion und eine AWS GovCloud (US) Version an.

Wenn Sie eine Produktintegration aktivieren, wird dem Produktabonnement automatisch eine Ressourcenrichtlinie angefügt. Diese Ressourcenrichtlinie definiert die Berechtigungen, die Security Hub CSPM benötigt, um Ergebnisse aus diesem Produkt zu erhalten.

Nachdem Sie alle vorbereitenden Schritte zur Aktivierung einer Integration abgeschlossen haben, können Sie den Fluss der Ergebnisse aus dieser Integration deaktivieren und wieder aktivieren. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen auf der Seite Integrationen an, ob Sie derzeit Ergebnisse akzeptieren.

Security Hub CSPM console

Um den Fluss von Erkenntnissen aus einer Integration (Konsole) zu ermöglichen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.
3. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen an, ob Security Hub CSPM derzeit Ergebnisse aus dieser Integration akzeptiert.
4. Wählen Sie Ergebnisse akzeptieren aus.

Security Hub CSPM API

Verwenden Sie die EnableImportFindingsForProductOperation. Wenn Sie den verwenden AWS CLI, führen Sie den enable-import-findings-for-productBefehl aus. Damit Security Hub Ergebnisse aus einer Integration empfangen kann, benötigen Sie das Produkt ARN. Verwenden Sie den Vorgang, um die ARNs für die verfügbaren Integrationen DescribeProductsabzurufen. Wenn Sie den verwenden AWS CLI, führen Sie den aus. describe-products

Mit dem folgenden AWS CLI Befehl kann Security Hub CSPM beispielsweise Ergebnisse aus der CrowdStrike Falcon-Integration empfangen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Deaktivierung des Erkenntnisflusses aus einer Security Hub CSPM-Integration

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Fluss der Ergebnisse aus einer AWS Security Hub CSPM-Integration zu deaktivieren.

Security Hub CSPM console

So deaktivieren Sie den Fluss der Ergebnisse aus einer Integration (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.
3. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen an, ob Security Hub CSPM derzeit Ergebnisse aus dieser Integration akzeptiert.
4. Wählen Sie Beenden der Annahme von Ergebnissen.

Security Hub CSPM API

Verwenden Sie die DisableImportFindingsForProductOperation. Wenn Sie den verwenden AWS CLI, führen Sie den disable-import-findings-for-productBefehl aus. Um den Fluss der Ergebnisse einer Integration zu deaktivieren, benötigen Sie den Abonnement-ARN für die aktivierte Integration. Verwenden Sie den ListEnabledProductsForImportVorgang, um den Abonnement-ARN zu erhalten. Wenn Sie den verwenden AWS CLI, führen Sie den aus list-enabled-products-for-import.

Der folgende AWS CLI Befehl deaktiviert beispielsweise den Fluss von Ergebnissen aus der Falcon-Integration an Security Hub CSPM. CrowdStrike Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Ergebnisse einer Security Hub CSPM-Integration anzeigen

Wenn Sie beginnen, Ergebnisse aus einer AWS Security Hub CSPM-Integration zu akzeptieren, zeigt die Seite Integrationen der Security Hub CSPM-Konsole den Status der Integration als Ergebnisse akzeptieren an. Um eine Liste der Ergebnisse der Integration einzusehen, wählen Sie Ergebnisse anzeigen.

Die Ergebnisliste zeigt die aktiven Ergebnisse für die ausgewählte Integration mit dem Workflow-Status `NEW` oder `NOTIFIED`.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthält die Liste in der Aggregationsregion Ergebnisse aus der Aggregationsregion und aus verknüpften Regionen, in denen die Integration aktiviert ist. Security Hub aktiviert Integrationen nicht automatisch, die auf der regionsübergreifenden Aggregationskonfiguration basieren.

In anderen Regionen enthält die Ergebnisliste für eine Integration nur Ergebnisse aus der aktuellen Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter. the section called “Aggregation von Daten über Regionen hinweg”

In der Ergebnisliste können Sie die folgenden Aktionen ausführen.

- Ändern der Filter und Gruppierung für die Liste
- Anzeigen der Details für einzelne Ergebnisse
- Aktualisieren des Workflow-Status der Ergebnisse
- Senden der Ergebnisse an benutzerdefinierte Aktionen

AWS-Service Integrationen mit Security Hub CSPM

AWS Security Hub CSPM unterstützt Integrationen mit mehreren anderen. AWS-Services Diese Integrationen können Ihnen helfen, sich einen umfassenden Überblick über Sicherheit und Compliance in Ihrer gesamten Umgebung zu verschaffen. AWS

Sofern unten nicht anders angegeben, werden AWS-Service Integrationen, die Ergebnisse an Security Hub CSPM senden, automatisch aktiviert, nachdem Sie Security Hub CSPM und den anderen Dienst aktiviert haben. Integrationen, die Security Hub CSPM-Ergebnisse erhalten, erfordern möglicherweise zusätzliche Schritte zur Aktivierung. Lesen Sie die Informationen zu den einzelnen Integrationen, um mehr zu erfahren.

Einige Integrationen sind nicht in allen AWS-Regionen verfügbar. Auf der Security Hub CSPM-Konsole wird eine Integration nicht auf der Seite Integrationen angezeigt, wenn sie in der aktuellen Region nicht unterstützt wird. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unterVerfügbarkeit von Integrationen nach Regionen.

Überblick über AWS Serviceintegrationen mit Security Hub CSPM

Die folgende Tabelle bietet einen Überblick über AWS Dienste, die Ergebnisse an Security Hub CSPM senden oder Ergebnisse von Security Hub CSPM empfangen.

Integrierter Service AWS	Richtung	
AWS Config	Sendet Ergebnisse	

Integrierter Service AWS	Richtung
AWS Firewall Manager	Sendet Ergebnisse
Amazon GuardDuty	Sendet Ergebnisse
AWS Health	Sendet Ergebnisse
AWS Identity and Access Management Access Analyzer	Sendet Ergebnisse
Amazon Inspector	Sendet Ergebnisse
AWS IoT Device Defender	Sendet Ergebnisse
Amazon Macie	Sendet Ergebnisse
Amazon Route 53 Resolver DNS-Firewall	Sendet Ergebnisse
AWS Systems Manager Patchmanager	Sendet Ergebnisse
AWS Audit Manager	Empfängt Ergebnisse
Amazon Q Developer in Chat-Anwendungen	Erhält Ergebnisse
Amazon Detective	Erhält Ergebnisse
Amazon Security Lake	Erhält Ergebnisse
AWS Systems Manager E ntdecker und OpsCenter	Empfängt und aktualisiert die Ergebnisse
AWS Trusted Advisor	Erhält Ergebnisse

AWS-Services die Ergebnisse an Security Hub CSPM senden

Die folgenden Funktionen AWS-Services lassen sich in Security Hub CSPM integrieren und können Ergebnisse an Security Hub CSPM senden. Security Hub CSPM konvertiert die Ergebnisse in das AWS Security Finding Format.

AWS Config (Sendet Ergebnisse)

AWS Config ist ein Service, mit dem Sie die Konfigurationen Ihrer AWS Ressourcen bewerten, prüfen und auswerten können. AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf und ermöglicht es Ihnen, die Auswertung der aufgezeichneten Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren.

Wenn Sie die Integration mit verwenden AWS Config, können Sie die Ergebnisse AWS Config verwalteter und benutzerdefinierter Regelauswertungen als Ergebnisse in Security Hub CSPM anzeigen. Diese Ergebnisse können zusammen mit anderen CSPM-Ergebnissen von Security Hub eingesehen werden und bieten so einen umfassenden Überblick über Ihren Sicherheitsstatus.

AWS Config verwendet Amazon EventBridge , um AWS Config Regelauswertungen an Security Hub CSPM zu senden. Security Hub CSPM wandelt die Regelauswertungen in Ergebnisse um, die dem AWS Security Finding Format entsprechen. Security Hub CSPM bereichert die Ergebnisse dann nach bestem Wissen und Gewissen, indem weitere Informationen über die betroffenen Ressourcen abgerufen werden, z. B. der Amazon-Ressourcenname (ARN), die Ressourcen-Tags und das Erstellungsdatum.

Weitere Informationen zu dieser Integration finden Sie in den folgenden Abschnitten.

Wie AWS Config sendet Ergebnisse an Security Hub CSPM

Alle Ergebnisse in Security Hub CSPM verwenden das standardmäßige JSON-Format von ASFF. ASFF enthält Details zur Herkunft des Befundes, zur betroffenen Ressource und zum aktuellen Status des Ergebnisses. AWS Config sendet verwaltete und benutzerdefinierte Regelauswertungen an Security Hub CSPM über. EventBridge Security Hub CSPM wandelt die Regelauswertungen in Ergebnisse um, die sich an ASFF orientieren, und bereichert die Ergebnisse nach bestem Wissen und Gewissen.

Arten von Ergebnissen, die AWS Config sendet an Security Hub CSPM

AWS Config Sendet nach der Aktivierung der Integration Bewertungen aller AWS Config verwalteten Regeln und benutzerdefinierten Regeln an Security Hub CSPM. Es werden nur Bewertungen gesendet, die nach der Aktivierung von Security Hub CSPM durchgeführt wurden. Nehmen wir

zum Beispiel an, dass bei einer AWS Config Regelauswertung fünf Ressourcen ausgefallen sind. Wenn Sie Security Hub CSPM nach dieser Bewertung aktivieren und die Regel dann eine sechste ausgefallene Ressource aufdeckt, wird nur die sechste Ressourcenbewertung an Security Hub CSPM AWS Config gesendet.

Evaluierungen anhand von serviceverknüpften AWS Config Regeln, wie sie beispielsweise zur Durchführung von Prüfungen auf Security Hub CSPM-Steuerelemente verwendet werden, sind ausgeschlossen. Eine Ausnahme bilden Ergebnisse, die durch serviceverknüpfte Regeln generiert wurden, die in AWS Control Tower erstellt und verwaltet werden. AWS Config Wenn Sie Ergebnisse für diese Regeln angeben, können Sie sicherstellen, dass Ihre Ergebnisdaten auch die Ergebnisse proaktiver Prüfungen enthalten, die von AWS Control Tower durchgeführt wurden.

Wird gesendet AWS Config Ergebnisse zu Security Hub CSPM

Wenn die Integration aktiviert ist, weist Security Hub CSPM automatisch die Berechtigungen zu, die für den Empfang von Ergebnissen erforderlich sind. AWS Config Security Hub CSPM verwendet Service-to-Service-Level-Berechtigungen, die Ihnen eine sichere Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse von Amazon zu importieren. AWS Config EventBridge

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Config erstellt wird, können Sie das Ergebnis normalerweise innerhalb von fünf Minuten in Security Hub CSPM anzeigen.

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

AWS Config sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub CSPM. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub CSPM übermittelt wurde, wird die Zustellung bis zu 24 Stunden oder 185 Mal EventBridge wiederholt, je nachdem, was zuerst eintritt.

Bestehende aktualisieren AWS Config Ergebnisse im Security Hub CSPM

Nachdem ein Ergebnis an Security Hub CSPM AWS Config gesendet wurde, kann es Aktualisierungen desselben Ergebnisses an Security Hub CSPM senden, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln. Updates werden nur für Ereignisse gesendet. `ComplianceChangeNotification` Wenn keine Änderung der Konformität erfolgt, werden keine Updates an Security Hub CSPM gesendet. Security Hub CSPM löscht Ergebnisse 90 Tage nach dem letzten Update oder 90 Tage nach der Erstellung, wenn kein Update erfolgt.

Security Hub CSPM archiviert keine Ergebnisse, die gesendet werden, AWS Config selbst wenn Sie die zugehörige Ressource löschen.

Regionen, in denen AWS Config Ergebnisse liegen vor

AWS Config Die Ergebnisse werden auf regionaler Basis getroffen. AWS Config sendet Ergebnisse an Security Hub CSPM in derselben Region oder Regionen, in denen die Ergebnisse auftreten.

Wird angezeigt AWS Config Ergebnisse im Security Hub CSPM

Um Ihre AWS Config Ergebnisse anzuzeigen, wählen Sie Findings im Security Hub CSPM-Navigationsbereich aus. Um die Ergebnisse so zu filtern, dass nur AWS Config Ergebnisse angezeigt werden, wählen Sie in der Dropdownliste der Suchleiste die Option Produktname aus. Geben Sie Config ein und wählen Sie Apply aus.

Dolmetschen AWS Config Namen in Security Hub CSPM suchen

Security Hub CSPM wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem folgen. AWS Format für Sicherheitssuche (ASFF) AWS Config Regelauswertungen verwenden im Vergleich zu ASFF ein anderes Ereignismuster. In der folgenden Tabelle werden die Felder für die AWS Config Regelauswertung ihrem ASFF-Gegenstück zugeordnet, so wie sie in Security Hub CSPM erscheinen.

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
detail.aws AccountId	AwsAccountId	
detail.neu EvaluationResult.resultRecordedTime	CreatedAt	
detail.neu EvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region >„arn: :securityhub::: /config“ product/aws
	ProductName	„Config“
	CompanyName	"AWS"
	Region	„eu-central-1"
Konfiguration RuleArn	GeneratorId, ProductFields	

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
Detail. ConfigRuleARN/finding/hash	Id	
detail.config RuleName	Titel, ProductFields	
detail.config RuleName	Description	„Dieses Ergebnis wurde für eine Änderung der Ressourcenkonformität für die Konfigurationsregel erstellt: “ `${detail.ConfigRuleName}`
Konfigurationselement „ARN“ oder von Security Hub CSPM berechneter ARN	Ressourcen [i] .id	
detail.Ressourcentyp	Ressourcen [i] .Type	"AwsS3Bucket"
	Ressourcen [i] .Partition	"aws"
	Ressourcen [i] .Region	„eu-central-1"
Konfigurationselement „Konfiguration“	Ressourcen [i] .Details	
	SchemaVersion	„2018-10-08"
	Severity.Label	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“
	Typen	["Software- und Konfigurationsprüfungen"]

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
detail.neu EvaluationResult.complianceType	Compliance.Status	„FEHLGESCHLAGEN“, „NOT_AVAILABLE“, „BESTANDEN“ oder „WARNUNG“
	Workflow.Status	„RESOLVED“, wenn ein AWS Config Ergebnis mit einem Wert Compliance.Status von „PASSED“ generiert wird oder wenn Compliance.Status sich der Wert von „FAILED“ in „PASSED“ ändert. Andernfalls Workflow.Status wird es „NEU“ sein. Sie können diesen Wert mit der BatchUpdateFindingsAPI-Operation ändern.

Interpretation der Bezeichnung des Schweregrads

Alle Ergebnisse aus AWS Config Regelauswertungen haben in der ASFF standardmäßig den Schweregrad MITTEL. Sie können den Schweregrad eines Ergebnisses mit dem `BatchUpdateFindings`API-Vorgang aktualisieren.

Typischer Befund von AWS Config

Security Hub CSPM wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem ASFF folgen. Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis aus AWS Config der ASFF.

> **Note**
>
> Wenn die Beschreibung mehr als 1.024 Zeichen umfasst, wird sie auf 1.024 Zeichen gekürzt und am Ende steht „(gekürzt)“.

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
```

```
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. AWS Config beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

Um das Senden von Ergebnissen an Security Hub CSPM zu beenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Anweisungen zum Stoppen des Flusses von Ergebnissen finden Sie unter. Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen

AWS Firewall Manager (Sendet Ergebnisse)

Firewall Manager sendet Ergebnisse an Security Hub CSPM, wenn eine Web Application Firewall (WAF) -Richtlinie für Ressourcen oder eine Web Access Control List (Web ACL) -Regel nicht den Vorschriften entspricht. Firewall Manager sendet auch Erkenntnisse, wenn AWS Shield Advanced Ressourcen nicht geschützt sind oder wenn ein Angriff erkannt wird.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Firewall Manager beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie auf der Seite Integrationen in der Security Hub CSPM-Konsole.

Weitere Informationen zu Firewall Manager finden Sie im AWS WAF Entwicklerhandbuch.

Amazon GuardDuty (Sendet Ergebnisse)

GuardDuty sendet alle von ihm generierten Befundtypen an Security Hub CSPM. Für einige Befundtypen gelten Voraussetzungen, Aktivierungsanforderungen oder regionale Einschränkungen. Weitere Informationen GuardDuty finden Sie im GuardDuty Amazon-Benutzerhandbuch unter Typen suchen.

Neue Ergebnisse von GuardDuty werden innerhalb von fünf Minuten an Security Hub CSPM gesendet. Aktualisierungen der Ergebnisse werden auf der Grundlage der Einstellung Aktualisierte Ergebnisse für Amazon EventBridge in den GuardDuty Einstellungen gesendet.

Wenn Sie GuardDuty Stichprobenergebnisse mithilfe der GuardDuty Einstellungsseite generieren, empfängt Security Hub CSPM die Probenergebnisse und lässt das Präfix `[Sample]` im Befundtyp weg. Beispielsweise GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` wird der Suchtyp der Stichprobe in wie `Recon:IAMUser/ResourcePermissions` in Security Hub CSPM angezeigt.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. GuardDutybeginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur GuardDuty Integration finden Sie unter Integration mit AWS Security Hub CSPM im GuardDuty Amazon-Benutzerhandbuch.

AWS Health (Sendet Ergebnisse)

AWS Health bietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer AWS-Services Ressourcen AWS-Konten. Sie können AWS Health Ereignisse verwenden, um zu erfahren, wie sich Änderungen an Diensten und Ressourcen auf Ihre Anwendungen auswirken können, die auf ausgeführt AWS werden.

Die Integration mit verwendet AWS Health nicht`BatchImportFindings`. AWS Health Verwendet stattdessen Service-to-Service-Event-Messaging, um Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie in den folgenden Abschnitten.

Wie AWS Health sendet Ergebnisse an Security Hub CSPM

In Security Hub CSPM werden Sicherheitsprobleme als Erkenntnisse verfolgt. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub CSPM verfügt außerdem über eine Reihe von Regeln, anhand derer Sicherheitsprobleme erkannt und Ergebnisse generiert werden.

Security Hub CSPM bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Siehe Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Siehe Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen.

Alle Ergebnisse in Security Hub CSPM verwenden ein Standard-JSON-Format namens. AWS Format für Sicherheitssuche (ASFF) ASFF enthält Einzelheiten zur Ursache des Problems, zu den betroffenen Ressourcen und zum aktuellen Stand der Ergebnisse.

AWS Health ist einer der AWS Dienste, der Ergebnisse an Security Hub CSPM sendet.

Arten von Ergebnissen, die AWS Health sendet an Security Hub CSPM

AWS Health Sendet nach der Aktivierung der Integration Ergebnisse, die eine oder mehrere der aufgelisteten Spezifikationen erfüllen, an Security Hub CSPM. Security Hub CSPM nimmt die Ergebnisse in die auf. AWS Format für Sicherheitssuche (ASFF)

- Ergebnisse, die einen der folgenden Werte enthalten für: AWS-Service
  - `RISK`
  - `ABUSE`
  - `ACM`
  - `CLOUDHSM`
  - `CLOUDTRAIL`
  - `CONFIG`
  - `CONTROLTOWER`
  - `DETECTIVE`
  - `EVENTS`
  - `GUARDDUTY`
  - `IAM`

- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB

- Ergebnisse mit den Wörtern `securityabuse`, oder `certificate` im AWS Health `typeCode` Feld
- Feststellungen, wo sich der AWS Health Dienst befindet `risk` oder `abuse`

Senden AWS Health Ergebnisse zu Security Hub CSPM

Wenn Sie sich dafür entscheiden, Ergebnisse von zu akzeptieren AWS Health, weist Security Hub CSPM automatisch die Berechtigungen zu, die für den Empfang der Ergebnisse von erforderlich sind. AWS Health Security Hub CSPM verwendet Service-to-Service-Level-Berechtigungen, die Ihnen eine sichere und einfache Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse von AWS Health Amazon EventBridge in Ihrem Namen zu importieren. Wenn Sie „Ergebnisse akzeptieren“ wählen, erteilt Security Hub CSPM die Erlaubnis, Ergebnisse von zu verwenden. AWS Health

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Health erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub CSPM gesendet.

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

AWS Health sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub CSPM. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub CSPM übermittelt wurde, wird EventBridge erneut versucht, das Ereignis für 24 Stunden zu senden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub CSPM

Nachdem ein Ergebnis an Security Hub CSPM AWS Health gesendet wurde, kann es Updates zu demselben Ergebnis senden, um zusätzliche Beobachtungen der Findungsaktivität an Security Hub CSPM widerzuspiegeln.

Regionen, in denen Ergebnisse vorliegen

AWS Health Sendet bei globalen Ereignissen Ergebnisse an Security Hub CSPM in us-east-1 (AWS Partition), cn-northwest-1 (Partition China) und gov-us-west-1 (Partition). GovCloud AWS Health sendet Region-specific Ereignisse an Security Hub CSPM in derselben Region oder Regionen, in denen die Ereignisse auftreten.

Wird angezeigt AWS Health Ergebnisse im Security Hub CSPM

Um Ihre AWS Health Ergebnisse in Security Hub CSPM anzuzeigen, wählen Sie im Navigationsbereich Findings aus. Um die Ergebnisse so zu filtern, dass nur AWS Health Ergebnisse angezeigt werden, wählen Sie Health aus dem Feld Produktname aus.

Dolmetschen AWS Health Namen in Security Hub CSPM suchen

AWS Health sendet die Ergebnisse mit dem an Security Hub CSPM. AWS Format für Sicherheitssuche (ASFF) AWS Health Die Suche verwendet ein anderes Ereignismuster als das

Security Hub CSPM ASFF-Format. In der folgenden Tabelle sind alle Ergebnisfelder mit ihren ASFF-Gegenstücken aufgeführt, so wie sie in Security Hub CSPM erscheinen. AWS Health

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
Konto	AwsAccountId	
Detail.StartTime	CreatedAt	
detail.Ereignis Description.latestDescription	Description	
detail.veranstaltung TypeCode	GeneratorId	
detail.eventArn (einschließlich Konto) + Hash von detail.startTime	Id	
<region>„arn:aws:securityhub::: /health“ product/aws	ProductArn	
Konto oder resourceId	Ressourcen [i] .id	
	Ressourcen [i] .Type	„Andere“
	SchemaVersion	„2018-10-08"
	Severity.Label	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“
„AWS Health -“ detail.event TypeCode	Title	
-	Typen	["Software- und Konfigurationsprüfungen"]
event.time	UpdatedAt	

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
URL des Ereignisses auf der Health Console	SourceUrl	

Der Schweregrad wird interpretiert

Der Schweregrad im ASFF-Ergebnis wird anhand der folgenden Logik bestimmt:

- Schweregrad KRITISCH wenn:
  - Das `service` Feld im AWS Health Ergebnis hat den Wert `Risk`
  - Das `typeCode` Feld im AWS Health Ergebnis hat den Wert `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - Das `typeCode` Feld im AWS Health Ergebnis hat den Wert `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - Das `typeCode` Feld im AWS Health Ergebnis hat den Wert `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  Schweregrad HOCH, wenn:
  - Das `service` Feld im AWS Health Ergebnis hat den Wert `Abuse`
  - Das `typeCode` Feld im AWS Health Befund enthält den Wert `SECURITY_NOTIFICATION`
  - Das `typeCode` Feld im AWS Health Befund enthält den Wert `ABUSE_DETECTION`

  Schweregrad MITTEL, wenn:
  - Das `service` Feld im Ergebnis ist eines der folgenden:`ACM`,,,,,`ARTIFACT`,,`AUDITMANAGER`,`BACKUP`,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`,,`CLOUD` oder `WAF`
  - Das TypeCode-Feld im AWS Health Ergebnis enthält den Wert `CERTIFICATE`
  - Das TypeCode-Feld im AWS Health Befund enthält den Wert `END_OF_SUPPORT`

Typischer Befund von AWS Health

AWS Health sendet Ergebnisse mit dem an Security Hub CSPM. AWS Format für Sicherheitssuche (ASFF) Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis von. AWS Health

> **Note**
>
> Wenn die Beschreibung mehr als 1024 Zeichen umfasst, wird sie auf 1024 Zeichen gekürzt und am Ende steht (gekürzt).


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
```

```
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. AWS Health beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

Um das Senden von Ergebnissen an Security Hub CSPM zu beenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Anweisungen zum Stoppen des Flusses von Ergebnissen finden Sie unter. Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen

AWS Identity and Access Management Access Analyzer (Sendet Ergebnisse)

Mit IAM Access Analyzer werden alle Ergebnisse an Security Hub CSPM gesendet.

IAM Access Analyzer analysiert anhand von logischer Argumentation ressourcenbasierte Richtlinien, die auf unterstützte Ressourcen in Ihrem Konto angewendet werden. IAM Access Analyzer generiert ein Ergebnis, wenn er eine Richtlinienaussage entdeckt, die einem externen Principal den Zugriff auf eine Ressource in Ihrem Konto ermöglicht.

In IAM Access Analyzer kann nur das Administratorkonto Ergebnisse für Analyzer sehen, die für eine Organisation gelten. Bei Organisationsanalyseprogrammen gibt das `AwsAccountId` ASFF-Feld die Administratorkonto-ID an. Das `ResourceOwnerAccount` Feld `ProductFields` darunter gibt das Konto an, in dem das Ergebnis entdeckt wurde. Wenn Sie Analyzer für jedes Konto einzeln aktivieren, generiert Security Hub CSPM mehrere Ergebnisse, eines, das die Administratorkonto-ID identifiziert, und eines, das die Ressourcenkonto-ID identifiziert.

Weitere Informationen finden Sie unter Integration mit AWS Security Hub CSPM im IAM-Benutzerhandbuch.

Amazon Inspector (Sendet Ergebnisse)

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Schwachstellen überprüft. Amazon Inspector erkennt und scannt automatisch Amazon EC2 EC2-Instances und Container-Images, die sich in der Amazon Elastic Container Registry befinden. Der Scan sucht nach Softwareschwachstellen und unbeabsichtigten Netzwerkbedrohungen.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Amazon Inspector beginnt sofort, alle Ergebnisse, die es generiert, an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie unter Integration mit AWS Security Hub CSPM im Amazon Inspector Inspector-Benutzerhandbuch.

Security Hub CSPM kann auch Ergebnisse von Amazon Inspector Classic erhalten. Amazon Inspector Classic sendet Ergebnisse an Security Hub CSPM, die im Rahmen von Bewertungsläufen für alle unterstützten Regelpakete generiert wurden.

Weitere Informationen zur Integration finden Sie unter Integration mit AWS Security Hub CSPM im Amazon Inspector Classic-Benutzerhandbuch.

Die Ergebnisse für Amazon Inspector und Amazon Inspector Classic verwenden denselben Produkt-ARN. Die Ergebnisse von Amazon Inspector haben den folgenden Eintrag in`ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Von Amazon Inspector Code Security generierte Sicherheitsergebnisse sind für diese Integration nicht verfügbar. Sie können jedoch in der Amazon Inspector-Konsole und über die Amazon Inspector-API auf diese speziellen Ergebnisse zugreifen.

AWS IoT Device Defender (Sendet Ergebnisse)

AWS IoT Device Defender ist ein Sicherheitsdienst, der die Konfiguration Ihrer IoT-Geräte überprüft, angeschlossene Geräte überwacht, um ungewöhnliches Verhalten zu erkennen, und zur Minderung von Sicherheitsrisiken beiträgt.

Nachdem Sie AWS IoT Device Defender sowohl als auch Security Hub CSPM aktiviert haben, rufen Sie die Seite Integrationen der Security Hub CSPM-Konsole auf und wählen Sie Ergebnisse akzeptieren für Audit, Detect oder beides aus. AWS IoT Device Defender Audit and Detect beginnt, alle Ergebnisse an Security Hub CSPM zu senden.

AWS IoT Device Defender Audit sendet Prüfzusammenfassungen an Security Hub CSPM, die allgemeine Informationen für einen bestimmten Prüfungstyp und eine bestimmte Prüfungsaufgabe enthalten. AWS IoT Device Defender Detect sendet festgestellte Verstöße für maschinelles Lernen (ML), statistisches und statisches Verhalten an Security Hub CSPM. Audit sendet auch gefundene Updates an Security Hub CSPM.

Weitere Informationen zu dieser Integration finden Sie unter Integration mit AWS Security Hub CSPM im AWS IoT Entwicklerhandbuch.

Amazon Macie (Sendet Ergebnisse)

Amazon Macie ist ein Datensicherheitsservice, der sensible Daten mithilfe von Machine Learning und Musterabgleich entdeckt, Einblicke in Datensicherheitsrisiken bietet und automatischen Schutz vor diesen Risiken ermöglicht. Ein Ergebnis von Macie kann darauf hinweisen, dass in Ihrem Amazon S3 S3-Datenbestand ein potenzieller Richtlinienverstoß vorliegt oder sensible Daten vorhanden sind.

Nachdem Sie Security Hub CSPM aktiviert haben, beginnt Macie automatisch, Richtlinienergebnisse an Security Hub CSPM zu senden. Sie können die Integration so konfigurieren, dass auch Ergebnisse vertraulicher Daten an Security Hub CSPM gesendet werden.

In Security Hub CSPM wird der Suchtyp für eine Richtlinie oder einen Fund vertraulicher Daten auf einen Wert geändert, der mit ASFF kompatibel ist. Beispielsweise wird der `Policy:IAMUser/S3BucketPublic` Findungstyp in Macie wie `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` in Security Hub CSPM angezeigt.

Macie sendet auch generierte Probenergebnisse an Security Hub CSPM. Bei Stichprobenergebnissen lautet der Name der betroffenen Ressource `macie-sample-finding-bucket` und der Wert für das `Sample` Feld lautet. `true`

Weitere Informationen finden Sie unter Evaluierung der Macie-Ergebnisse mit Security Hub im Amazon Macie Macie-Benutzerhandbuch.

Amazon Route 53 Resolver DNS-Firewall (Sendet Ergebnisse)

Mit der Amazon Route 53 Resolver DNS-Firewall können Sie ausgehenden DNS-Verkehr für Ihre Virtual Private Cloud (VPC) filtern und regulieren. Dazu erstellen Sie wiederverwendbare Sammlungen von Filterregeln in DNS-Firewall-Regelgruppen, verknüpfen die Regelgruppen mit Ihrer VPC und überwachen dann die Aktivitäten in DNS-Firewallprotokollen und -Metriken. Je nach Aktivität können Sie das Verhalten der DNS-Firewall anpassen. Die DNS-Firewall ist eine Funktion von Route 53 Resolver.

Die Route 53 Resolver DNS Firewall kann verschiedene Arten von Ergebnissen an Security Hub CSPM senden:

- Ergebnisse im Zusammenhang mit Abfragen, bei denen es sich um blockierte oder Warnmeldungen für Domänen handelt, die AWS verwalteten Domänenlisten zugeordnet sind. AWS
- Ergebnisse im Zusammenhang mit Anfragen, die blockiert wurden oder bei denen eine Warnung ausgelöst wurde, für Domänen, die mit einer von Ihnen definierten, benutzerdefinierten Domänenliste verknüpft sind.
- Ergebnisse im Zusammenhang mit Abfragen, die von DNS Firewall Advanced blockiert wurden oder bei denen eine Warnung angezeigt wurde. Dabei handelt es sich um eine Route 53-Resolver-Funktion, mit der Abfragen im Zusammenhang mit komplexen DNS-Bedrohungen wie Domain Generation Algorithms (DGAs) und DNS-Tunneling erkannt werden können.

Nachdem Sie Security Hub CSPM und Route 53 Resolver DNS Firewall aktiviert haben, beginnt die DNS-Firewall automatisch, Ergebnisse für AWS verwaltete Domänenlisten und DNS Firewall Advanced an Security Hub CSPM zu senden. Um auch Ergebnisse für eine benutzerdefinierte

Domainliste an Security Hub CSPM zu senden, aktivieren Sie die Integration in Security Hub CSPM manuell.

In Security Hub CSPM haben alle Ergebnisse der Route 53 Resolver DNS Firewall den folgenden Typ:. `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Weitere Informationen finden Sie unter Senden von Ergebnissen von der Route 53 Resolver DNS Firewall an Security Hub im Amazon Route 53-Entwicklerhandbuch.

AWS Systems Manager Patch Manager (Sendet Ergebnisse)

AWS Systems Manager Patch Manager sendet Ergebnisse an Security Hub CSPM, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.

Patch Manager automatisiert das Patchen verwalteter Instances mit sicherheitsrelevanten und anderen Arten von Updates.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Systems Manager Patch Manager beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Verwendung von Patch Manager finden Sie unter AWS Systems Manager Patch Manager im AWS Systems Manager Benutzerhandbuch.

AWS Dienste, die Erkenntnisse von Security Hub CSPM erhalten

Die folgenden AWS Dienste sind in Security Hub CSPM integriert und beziehen Ergebnisse von Security Hub CSPM. Sofern angegeben, kann der integrierte Dienst die Ergebnisse auch aktualisieren. In diesem Fall wird das Auffinden von Updates, die Sie im integrierten Dienst vornehmen, auch in Security Hub CSPM widergespiegelt.

AWS Audit Manager (Erhält Ergebnisse)

AWS Audit Manager erhält Ergebnisse von Security Hub CSPM. Diese Ergebnisse helfen den Benutzern von Audit Manager, sich auf Audits vorzubereiten.

Weitere Informationen zu Audit Manager finden Sie im AWS Audit Manager Manager-Benutzerhandbuch. AWS Security Hub CSPM-Prüfungen, unterstützt von, AWS Audit Manager listet die Kontrollen auf, für die Security Hub CSPM Ergebnisse an Audit Manager sendet.

Amazon Q Developer in Chat-Anwendungen (erhält Ergebnisse)

Amazon Q Developer in Chat-Anwendungen ist ein interaktiver Agent, der Ihnen hilft, Ihre AWS Ressourcen in Ihren Slack-Kanälen und Amazon Chime Chime-Chatrooms zu überwachen und mit ihnen zu interagieren.

Amazon Q Developer in Chat-Anwendungen erhält Ergebnisse von Security Hub CSPM.

Weitere Informationen zur Integration von Amazon Q Developer in Chat-Anwendungen mit Security Hub CSPM finden Sie in der Übersicht über die Security Hub CSPM-Integration im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

Amazon Detective (erhält Ergebnisse)

Detective sammelt automatisch Protokolldaten aus Ihren AWS Ressourcen und nutzt maschinelles Lernen, statistische Analysen und Graphentheorie, um Sie bei der Visualisierung und Durchführung schnellerer und effizienterer Sicherheitsuntersuchungen zu unterstützen.

Die Security Hub CSPM-Integration mit Detective ermöglicht es Ihnen, von GuardDuty Amazon-Ergebnissen in Security Hub CSPM zu Detective zu wechseln. Anschließend können Sie die Detective-Tools und Visualisierungen verwenden, um sie zu untersuchen. Die Integration erfordert keine zusätzliche Konfiguration in Security Hub CSPM oder Detective.

Für Ergebnisse, die von anderen stammen AWS-Services, enthält der Bereich mit den Ergebnisdetails auf der Security Hub CSPM-Konsole den Unterabschnitt Investigate in Detective. Dieser Unterabschnitt enthält einen Link zu Detective, über den Sie das Sicherheitsproblem, das durch den Befund gemeldet wurde, weiter untersuchen können. Sie können in Detective auch ein Verhaltensdiagramm erstellen, das auf den Ergebnissen des Security Hub CSPM basiert, um effektivere Untersuchungen durchzuführen. Weitere Informationen finden Sie in den AWS Sicherheitsergebnissen im Amazon Detective Administration Guide.

Wenn die regionsübergreifende Aggregation aktiviert ist und Sie von der Aggregationsregion aus wechseln, wird Detective in der Region geöffnet, aus der das Ergebnis stammt.

Wenn ein Link nicht funktioniert, finden Sie Hinweise zur Fehlerbehebung unter Troubleshooting the Pivot.

Amazon Security Lake (erhält Ergebnisse)

Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Service. Sie können Security Lake verwenden, um Sicherheitsdaten aus Cloud-, lokalen und benutzerdefinierten Quellen automatisch in

einem Data Lake zu zentralisieren, der in Ihrem Konto gespeichert ist. Abonnenten können Daten aus Security Lake für Ermittlungs- und Analysezwecke nutzen.

Um diese Integration zu aktivieren, müssen Sie beide Dienste aktivieren und Security Hub CSPM als Quelle in der Security Lake-Konsole, der Security Lake-API oder hinzufügen. AWS CLI Sobald Sie diese Schritte abgeschlossen haben, beginnt Security Hub CSPM, alle Ergebnisse an Security Lake zu senden.

Security Lake normalisiert die CSPM-Ergebnisse von Security Hub automatisch und konvertiert sie in ein standardisiertes Open-Source-Schema namens Open Cybersecurity Schema Framework (OCSF). In Security Lake können Sie einen oder mehrere Abonnenten hinzufügen, um die CSPM-Ergebnisse von Security Hub zu nutzen.

Weitere Informationen zu dieser Integration, einschließlich Anweisungen zum Hinzufügen von Security Hub CSPM als Quelle und zum Erstellen von Abonnenten, finden Sie unter Integration mit AWS Security Hub CSPM im Amazon Security Lake-Benutzerhandbuch.

AWS Systems Manager Explorer und OpsCenter (Empfängt und aktualisiert Ergebnisse)

AWS Systems Manager Erkunden und OpsCenter empfangen Sie Ergebnisse von Security Hub CSPM und aktualisieren Sie diese Ergebnisse in Security Hub CSPM.

Explorer bietet Ihnen ein anpassbares Dashboard, das wichtige Einblicke und Analysen zum Betriebsstatus und zur Leistung Ihrer Umgebung bietet. AWS

OpsCenter bietet Ihnen einen zentralen Ort, an dem Sie betriebliche Arbeitsaufgaben anzeigen, untersuchen und lösen können.

Weitere Informationen zu Explorer und OpsCenter finden Sie unter Operations Management im AWS Systems Manager Benutzerhandbuch.

AWS Trusted Advisor (Erhält Ergebnisse)

Trusted Advisor stützt sich auf bewährte Verfahren, die bei der Betreuung von Hunderttausenden von AWS Kunden gelernt wurden. Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen.

Wenn Sie Trusted Advisor sowohl als auch Security Hub CSPM aktivieren, wird die Integration automatisch aktualisiert.

Security Hub CSPM sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an. Trusted Advisor

Weitere Informationen zur Security Hub CSPM-Integration mit Trusted Advisor finden Sie unter AWS Security Hub CSPM-Steuerelemente anzeigen AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

Third-party Produktintegrationen mit Security Hub CSPM

AWS Security Hub CSPM lässt sich in mehrere Partnerprodukte von Drittanbietern integrieren. Eine Integration kann eine oder mehrere der folgenden Aktionen ausführen:

- Senden Sie die generierten Ergebnisse an Security Hub CSPM
- Erhalten Sie Ergebnisse von Security Hub CSPM
- Ergebnisse im Security Hub CSPM aktualisieren

Integrationen, die Ergebnisse an Security Hub CSPM senden, haben einen Amazon-Ressourcennamen (ARN).

Eine Integration ist möglicherweise nicht in allen verfügbar. AWS-Regionen Wenn eine Integration in der Region, in der Sie derzeit angemeldet sind, auf der Security Hub CSPM-Konsole nicht unterstützt wird, wird sie nicht auf der Integrationsseite der Konsole angezeigt. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unterVerfügbarkeit von Integrationen nach Regionen.

`<Wenn Sie über eine Sicherheitslösung verfügen und daran interessiert sind, ein`
Weitere Informationen finden Sie im Leitfaden zur Partnerintegration.

Überblick über Integrationen von Drittanbietern mit Security Hub CSPM

Die folgende Tabelle bietet einen Überblick über die Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden oder Ergebnisse von Security Hub CSPM empfangen können.

Integration	Richtung	ARN (falls zutreffend)
3CORESec – 3CORESec NTA	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`

Integration	Richtung	ARN (falls zutreffend)
Alert Logic – SIEMless Threat Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere`
AttackIQ – AttackIQ	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform`
Barracuda Networks – Cloud Security Guardian	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Integration	Richtung	ARN (falls zutreffend)
BigID – BigID Enterprise	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise`
Blue Hexagon – Blue Hexagon forAWS	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws`
Check Point – CloudGuard IaaS	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas`
Check Point – CloudGuard Posture Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security—Antivirus for Amazon S3	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`
Contrast Security	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`

Integration	Richtung	ARN (falls zutreffend)
CrowdStrike – CrowdStrike Falcon	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`
Drata	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Integration	Richtung	ARN (falls zutreffend)
Forcepoint – Forcepoint DLP	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/fugue/fugue`
Guardicore – Centra 4.0	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Integration	Richtung	ARN (falls zutreffend)
k9 Security – Access Analyzer	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`
NETSCOUT – NETSCOUT Cyber Investigator	Sendet Ergebnisse	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`
Palo Alto Networks – Prisma Cloud Compute	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`

Integration	Richtung	ARN (falls zutreffend)
Plerion – Cloud Security Platform	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SentinelOne – SentinelOne	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Sendet Ergebnisse	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`

Integration	Richtung	ARN (falls zutreffend)
Sophos – Server Protection	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one

Integration	Richtung	ARN (falls zutreffend)
Vectra – Cognito Detect	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian - Jira Service Management Cloud	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian – Opsgenie	Erhält Ergebnisse	Nicht zutreffend
Dynatrace	Erhält Ergebnisse	Nicht zutreffend
Elastic	Erhält Ergebnisse	Nicht zutreffend
Fortinet – FortiCNP	Erhält Ergebnisse	Nicht zutreffend
IBM – QRadar	Erhält Ergebnisse	Nicht zutreffend
Logz.io Cloud SIEM	Erhält Ergebnisse	Nicht zutreffend
MetricStream	Erhält Ergebnisse	Nicht zutreffend
MicroFocus – MicroFocus Arcsight	Erhält Ergebnisse	Nicht zutreffend
New Relic Vulnerability Management	Erhält Ergebnisse	Nicht zutreffend
PagerDuty – PagerDuty	Erhält Ergebnisse	Nicht zutreffend

Integration	Richtung	ARN (falls zutreffend)
Palo Alto Networks – Cortex XSOAR	Erhält Ergebnisse	Nicht zutreffend
Palo Alto Networks – VM-Series	Erhält Ergebnisse	Nicht zutreffend
Rackspace Technology – Cloud Native Security	Erhält Ergebnisse	Nicht zutreffend
Rapid7 – InsightConnect	Erhält Ergebnisse	Nicht zutreffend
RSA – RSA Archer	Erhält Ergebnisse	Nicht zutreffend
ServiceNow – ITSM	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Slack – Slack	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Enterprise	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Phantom	Erhält Ergebnisse	Nicht zutreffend
ThreatModeler	Erhält Ergebnisse	Nicht zutreffend
Trellix – Trellix Helix	Erhält Ergebnisse	Nicht zutreffend
Caveonix – Caveonix Cloud	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`

Integration	Richtung	ARN (falls zutreffend)
DisruptOps, Inc. – DisruptOPS	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Third-party Integrationen, die Ergebnisse an Security Hub CSPM senden

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse an Security Hub CSPM senden. Security Hub CSPM wandelt die Ergebnisse in das AWS Security Finding Format um.

3 CoreSec – 3 CoreSec NTA

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecbietet verwaltete Erkennungsdienste sowohl für lokale Umgebungen als auch für AWS Systeme. Ihre Integration mit Security Hub CSPM ermöglicht Einblicke in Bedrohungen wie Malware, Rechteausweitung, laterale Bewegungen und unsachgemäße Netzwerksegmentierung.

Link zum Produkt

Dokumentation für Partner

Alert Logic – Bedrohungsmanagement ohne SIEM

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Sorgen Sie für das richtige Maß an Schutz: Sichtbarkeit von Schwachstellen und Ressourcen, Bedrohungserkennung und Vorfallmanagement sowie zugewiesene SOC-Analystenoptionen. AWS WAF

Link zum Produkt

Dokumentation für Partner

Aqua Security – Aqua Cloud Native Security Platform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)bietet Sicherheit über den gesamten Lebenszyklus von containerbasierten und serverlosen Anwendungen, von Ihrer CI/CD Pipeline bis hin zu Runtime-Produktionsumgebungen.

Link zum Produkt

Dokumentation für Partner

Aqua Security – Kube-bench

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchist ein Open-Source-Tool, das den Kubernetes-Benchmark des Center for Internet Security (CIS) in Ihrer Umgebung ausführt.

Link zum Produkt

Dokumentation für Partner

Armor – Armor Anywhere

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherebietet verwaltete Sicherheit und Compliance für AWS.

Link zum Produkt

Dokumentation für Partner

AttackIQ – AttackIQ

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformemuliert echtes gegnerisches Verhalten im Einklang mit dem MITRE ATT&CK Framework, um Ihre allgemeine Sicherheitslage zu validieren und zu verbessern.

Link zum Produkt

Dokumentation für Partner

Barracuda Networks – Cloud Security Guardian

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentryhilft Unternehmen dabei, beim Erstellen von Anwendungen in der Public Cloud und beim Verschieben von Workloads in die Public Cloud sicher zu bleiben.

AWS Link zum Marketplace

Link zum Produkt

BigID – BigID Enterprise

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

Das BigID Enterprise Privacy Management Platform hilft Unternehmen dabei, sensible Daten (PII) in all ihren Systemen zu verwalten und zu schützen.

Link zum Produkt

Dokumentation für Partner

Blaues Sechseck – Blaues Sechseck for AWS

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonist eine Plattform zur Erkennung von Bedrohungen in Echtzeit. Sie verwendet Deep-Learning-Prinzipien, um bekannte und unbekannte Bedrohungen, einschließlich Malware und Netzwerkanomalien, zu erkennen.

AWS Link zum Marketplace

Dokumentation für Partner

Checkpoint – CloudGuard IaaS

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuarderweitert auf einfache Weise die umfassende Sicherheit zur Bedrohungsabwehr AWS und schützt gleichzeitig Ressourcen in der Cloud.

Link zum Produkt

Dokumentation für Partner

Checkpoint – CloudGuard Verwaltung der Körperhaltung

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Eine SaaS-Plattform, die überprüfbare Cloud-Netzwerksicherheit, fortschrittlichen IAM-Schutz sowie umfassende Compliance und Governance bietet.

Link zum Produkt

Dokumentation für Partner

Klarheit – Kuppel

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomehilft Unternehmen dabei, ihre cyberphysischen Systeme im erweiterten Internet der Dinge (XIoT) in industriellen (OT), Gesundheits- (IoMT) und Unternehmensumgebungen (IoT) zu schützen.

Link zum Produkt

Dokumentation für Partner

Cloud-Speichersicherheit – Antivirus für Amazon S3

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securitybietet Cloud-native Anti-Malware- und Antivirenscans für Amazon S3 S3-Objekte.

Antivirus for Amazon S3 bietet Echtzeit- und geplante Scans von Objekten und Dateien in Amazon S3 auf Malware und Bedrohungen. Es bietet Transparenz und Problembehebung bei problematischen und infizierten Dateien.

Link zum Produkt

Dokumentation für Partner

Contrast Security — Contrast Assess

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessist ein IAST-Tool, das die Erkennung von Sicherheitslücken in Web-Apps, APIs und Microservices in Echtzeit ermöglicht. Contrast Assesslässt sich in Security Hub CSPM integrieren, um zentrale Transparenz und Reaktionsfähigkeit für all Ihre Workloads zu gewährleisten.

Link zum Produkt

Dokumentation für Partner

CrowdStrike – CrowdStrike Falcon

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Der CrowdStrike Falcon einzelne, leichte Sensor vereint Virenschutz der nächsten Generation, Erkennung und Reaktion auf Endgeräte sowie 24/7 verwaltetes Hunting über die Cloud.

AWS Link zum Marketplace

Dokumentation für Partner

CyberArk – Privileged Threat Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat AnalyticsErfassung, Erkennung und Reaktion auf risikoreiche Aktivitäten und Verhaltensweisen privilegierter Konten, um laufende Angriffe einzudämmen.

Link zum Produkt

Dokumentation für Partner

Satz von Daten – Satz von Daten

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremscannt kontinuierlich Webanwendungen, APIs und Cloud-Ressourcen auf der Suche nach Sicherheitslücken und Datenschutzlücken, um AppSec Datenschutzverletzungen zu verhindern.

Link zum Produkt

Dokumentation für Partner

Daten

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataist eine Plattform zur Compliance-Automatisierung, mit der Sie die Einhaltung verschiedener Frameworks wie SOC2, ISO und GDPR erreichen und aufrechterhalten können. Die Integration zwischen Drata und Security Hub CSPM hilft Ihnen, Ihre Sicherheitserkenntnisse an einem Ort zu zentralisieren.

AWS Link zum Marketplace

Dokumentation für Partner

Forcepoint – Forcepoint CASB

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBermöglicht es Ihnen, die Nutzung von Cloud-Anwendungen zu ermitteln, Risiken zu analysieren und angemessene Kontrollen für SaaS- und benutzerdefinierte Anwendungen durchzusetzen.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint Cloud Security Gateway

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayist ein konvergenter Cloud-Sicherheitsdienst, der Transparenz, Kontrolle und Bedrohungsschutz für Benutzer und Daten bietet, egal wo sie sich befinden.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint DLP

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPbegegnet Risiken, bei denen der Mensch im Mittelpunkt steht, und bietet Transparenz und Kontrolle überall dort, wo Ihre Mitarbeiter arbeiten und wo sich Ihre Daten befinden.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint NGFW

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWermöglicht es Ihnen, Ihre AWS Umgebung mit Ihrem Unternehmensnetzwerk zu verbinden und bietet die Skalierbarkeit, den Schutz und die Einblicke, die Sie benötigen, um Ihr Netzwerk zu verwalten und auf Bedrohungen zu reagieren.

Link zum Produkt

Dokumentation für Partner

Fuge – Fuge

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueist eine skalierbare Cloud-native Plattform ohne Agenten, die die kontinuierliche Validierung von Infrastructure-as-Code- und Cloud-Runtime-Umgebungen unter Verwendung derselben Richtlinien automatisiert.

Link zum Produkt

Dokumentation für Partner

Guardicore – Centra 4.0

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centrabietet Flussvisualisierung, Mikrosegmentierung und Erkennung von Sicherheitslücken für Workloads in modernen Rechenzentren und Clouds.

Link zum Produkt

Dokumentation für Partner

HackerOne – Informationen zu Sicherheitslücken

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

Die HackerOne Plattform arbeitet mit der weltweiten Hacker-Community zusammen, um die wichtigsten Sicherheitsprobleme aufzudecken. Vulnerability Intelligenceermöglicht es Ihrem Unternehmen, über automatisiertes Scannen hinauszugehen. Es enthält Sicherheitslücken, die von HackerOne ethischen Hackern validiert und Schritte zur Reproduktion bereitgestellt wurden.

AWS Link zum Marktplatz

Dokumentation für Partner

JFrog – Röntgen

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayist ein universelles Tool zur Analyse der Anwendungssicherheit (Software Composition Analysis, SCA), das Binärdateien kontinuierlich auf Lizenzbestimmungen und Sicherheitslücken scannt, sodass Sie eine sichere Software-Lieferkette betreiben können.

AWS Link zum Marketplace

Dokumentation für Partner

Juniper Networks – vSRX-Firewall der nächsten Generation

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRX Virtual Next Generation Firewall bietet eine vollständige cloudbasierte virtuelle Firewall mit erweiterter Sicherheit, sicheren SD-WAN, robusten Netzwerken und integrierter Automatisierung.

AWS Link zum Marketplace

Dokumentation für Partner

Link zum Produkt

k9 Sicherheit – Access Analyzer

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securitybenachrichtigt Sie, wenn wichtige Zugangsänderungen in Ihrem AWS Identity and Access Management Konto vorgenommen werden. Damit können Sie nachvollziehenk9 Security, welchen Zugriff Benutzer und IAM-Rollen auf wichtige Daten AWS-Services und Ihre Daten haben.

k9 Securityist für Continuous Delivery konzipiert und ermöglicht es Ihnen, IAM mit umsetzbaren Zugriffsprüfungen und einfacher Richtlinienautomatisierung für und Terraform zu operationalisieren. AWS CDK

Link zum Produkt

Dokumentation für Partner

Schnürsenkelarbeit – Schnürsenkel

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkist die datengesteuerte Sicherheitsplattform für die Cloud. Die Lacework Cloud Security Platform automatisiert Cloud-Sicherheit in großem Maßstab, sodass Sie schnell und sicher innovieren können.

Link zum Produkt

Dokumentation für Partner

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)bietet Cloud Security Posture Management (CSPM) und Cloud Workload Protection Platform (CWPP) für Ihre Umgebung. AWS

Link zum Produkt

Dokumentation für Partner

NETSCOUT – NETSCOUT Cyber-Ermittler

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatorist eine unternehmensweite Plattform für Netzwerkbedrohungen, Risikountersuchungen und forensische Analysen, die dazu beiträgt, die Auswirkungen von Cyberbedrohungen auf Unternehmen zu verringern.

Link zum Produkt

Dokumentation für Partner

Orca Cloud-Sicherheitsplattform

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Das Orca Cloud Security Platform identifiziert, priorisiert und behebt Risiken und Compliance-Probleme in Ihrer gesamten Cloud-Umgebung. Orca'sDie AI-driven Plattform ohne Agenten bietet umfassenden Schutz bei der Erkennung von Sicherheitslücken, Fehlkonfigurationen, lateralen Bewegungen, API-Risiken, sensiblen Daten, anomalen Ereignissen und Verhaltensweisen sowie übermäßig freizügigen Identitäten.

Orcalässt sich in Security Hub CSPM integrieren, um Deep-Cloud-Sicherheitstelemetrie in Security Hub CSPM zu integrieren. Orcasetzt seine SideScanning Technologie ein und priorisiert Risiken in Bezug auf Cloud-Infrastruktur, Workloads, Anwendungen, Daten, APIs, Identitäten und mehr.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Prisma Cloud Compute

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeist eine Cloud-native Cybersicherheitsplattform, die VMs, Container und serverlose Plattformen schützt.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Prisma Cloud Enterprise

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Schützt Ihre AWS Bereitstellung mit Cloud-Sicherheitsanalysen, fortschrittlicher Bedrohungserkennung und Compliance-Überwachung.

Link zum Produkt

Dokumentation für Partner

Plerion – Cloud-Sicherheitsplattform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionist eine Cloud-Sicherheitsplattform mit einem einzigartigen, bedrohungsorientierten, risikoorientierten Ansatz, der präventive, detektive und korrektive Maßnahmen für Ihre Workloads bietet. Die Integration zwischen Plerion und Security Hub CSPM ermöglicht es Kunden, ihre Sicherheitsergebnisse an einem Ort zu zentralisieren und entsprechend zu handeln.

AWS Link zum Marketplace

Dokumentation für Partner

Prowler – Herumtreiber

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowlerist ein Open-Source-Sicherheitstool zur Durchführung von AWS Prüfungen in Bezug auf bewährte Sicherheitsverfahren, Abhärtung und kontinuierliche Überwachung.

Link zum Produkt

Dokumentation für Partner

Qualys – Management von Schwachstellen

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)scannt und identifiziert kontinuierlich Sicherheitslücken und schützt so Ihre Ressourcen.

Link zum Produkt

Dokumentation für Partner

Rapid7 – InsightVM

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVMbietet Schwachstellenmanagement für moderne Umgebungen, sodass Sie Sicherheitslücken effizient finden, priorisieren und beheben können.

Link zum Produkt

Dokumentation für Partner

SentinelOne – SentinelOne

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneist eine autonome XDR-Plattform (Extended Detection and Response), die AI-powered Prävention, Erkennung, Reaktion und Suche über Endpunkte, Container, Cloud-Workloads und IoT-Geräte hinweg umfasst.

AWS Link zum Marketplace

Link zum Produkt

Snyk

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykbietet eine Sicherheitsplattform, die App-Komponenten auf Sicherheitsrisiken in Workloads überprüft, auf AWS denen sie ausgeführt werden. Diese Risiken werden als Ergebnisse an Security Hub CSPM gesendet, sodass Entwickler und Sicherheitsteams sie zusammen mit den übrigen Sicherheitsergebnissen visualisieren und priorisieren können AWS .

AWS Link zum Marketplace

Dokumentation für Partner

Sonari-Sicherheit – Sonrai Dig

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digüberwacht und behebt Cloud-Fehlkonfigurationen und Richtlinienverstöße, sodass Sie Ihren Sicherheits- und Compliance-Status verbessern können.

Link zum Produkt

Dokumentation für Partner

Sophos – Server Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectionschützt die kritischen Anwendungen und Daten, die das Herzstück Ihres Unternehmens bilden, mithilfe umfassender Techniken zur Tiefenabwehr.

Link zum Produkt

StackRox – StackRox Kubernetes-Sicherheit

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxhilft Unternehmen dabei, ihre Container- und Kubernetes-Implementierungen in großem Umfang zu sichern, indem sie ihre Compliance- und Sicherheitsrichtlinien über den gesamten Container-Lebenszyklus hinweg durchsetzen — bei der Erstellung, Bereitstellung und Ausführung.

Link zum Produkt

Dokumentation für Partner

Sumo Logic – Machine Data Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicist eine sichere Plattform zur Analyse von Maschinendaten, mit der Entwicklungs- und Sicherheitsteams ihre AWS Anwendungen erstellen, ausführen und sichern können.

Link zum Produkt

Dokumentation für Partner

Symantec – Cloud Workload Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionbietet umfassenden Schutz für Ihre Amazon EC2 EC2-Instances mit Malware-Schutz, Intrusion Prevention und Überwachung der Dateiintegrität.

Link zum Produkt

Dokumentation für Partner

Tenable – Tenable.io

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Präzises Identifizieren, Untersuchen und Priorisieren von Schwachstellen. In der Cloud verwaltet.

Link zum Produkt

Dokumentation für Partner

Trend Micro – Cloud One

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onestellt Teams zur richtigen Zeit und am richtigen Ort die richtigen Sicherheitsinformationen zur Verfügung. Diese Integration sendet Sicherheitsergebnisse in Echtzeit an Security Hub CSPM und verbessert so die Sichtbarkeit Ihrer AWS Ressourcen und Trend Micro Cloud One Ereignisdetails in Security Hub CSPM.

AWS Link zum Marketplace

Dokumentation für Partner

Vectra – Cognito Detect

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectraverändert die Cybersicherheit, indem es fortschrittliche KI einsetzt, um versteckte Cyberangreifer zu erkennen und darauf zu reagieren, bevor sie stehlen oder Schaden anrichten können.

AWS Link zum Marketplace

Dokumentation für Partner

Wiz – Wiz-Sicherheit

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanalysiert kontinuierlich Konfigurationen, Sicherheitslücken, Netzwerke, IAM-Einstellungen, Geheimnisse und mehr für Sie AWS-Konten, Benutzer und Workloads, um kritische Probleme zu

entdecken, die ein echtes Risiko darstellen. Integrieren Sie Wiz in Security Hub CSPM, um Probleme zu visualisieren und darauf zu reagieren, die Wiz von der Security Hub CSPM-Konsole aus erkennt.

AWS Link zum Marketplace

Dokumentation für Partner

Third-party Integrationen, die Erkenntnisse von Security Hub CSPM erhalten

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse von Security Hub CSPM erhalten. Sofern angegeben, aktualisiert das Produkt möglicherweise auch die Ergebnisse. In diesem Fall werden Aktualisierungen, die Sie an den Ergebnissen des Partnerprodukts vornehmen, auch in Security Hub CSPM widergespiegelt.

Atlassian - Jira Service Management

Integrationstyp: Empfangen und aktualisieren

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub CSPM an. Jira JiraProbleme werden auf der Grundlage der Ergebnisse erstellt. Wenn die Jira Probleme aktualisiert werden, werden die entsprechenden Ergebnisse in Security Hub CSPM aktualisiert.

Die Integration unterstützt nur Jira Server und Jira Data Center.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video AWS Security Hub CSPM — Bidirektionale Integration mit. Atlassian Jira Service Management

Link zum Produkt

Dokumentation für Partner

Atlassian - Jira Service Management Cloud

Integrationstyp: Empfangen und aktualisieren

Jira Service Management Cloudist die Cloud-Komponente von Jira Service Management.

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub CSPM an. Jira Die Ergebnisse lösen die Entstehung von Problemen in aus. Jira Service Management Cloud Wenn Sie diese Probleme in aktualisierenJira Service Management Cloud, werden die entsprechenden Ergebnisse auch in Security Hub CSPM aktualisiert.

Link zum Produkt

Dokumentation für Partner

Atlassian – Opsgenie

Integrationstyp: Empfangen

Opsgenieist eine moderne Incident-Management-Lösung für den Betrieb ständig verfügbarer Dienste, die es Entwicklungs- und Betriebsteams ermöglicht, Serviceunterbrechungen zu planen und bei Vorfällen die Kontrolle zu behalten.

Durch die Integration mit Security Hub CSPM wird sichergestellt, dass geschäftskritische sicherheitsrelevante Vorfälle zur sofortigen Lösung an die entsprechenden Teams weitergeleitet werden.

Link zum Produkt

Dokumentation für Partner

Dynatrace

Integrationstyp: Empfangen

Die Dynatrace Integration mit Security Hub CSPM hilft dabei, Sicherheitserkenntnisse in allen Tools und Umgebungen zu vereinheitlichen, zu visualisieren und zu automatisieren. Das Hinzufügen von Dynatrace Laufzeitkontexten zu den Sicherheitsergebnissen ermöglicht eine intelligentere Priorisierung, trägt dazu bei, die durch Warnmeldungen verursachten Störungen zu reduzieren und Ihre DevSecOps Teams darauf zu konzentrieren, die kritischen Probleme, die Ihre Produktionsumgebungen und Anwendungen betreffen, effizient zu beheben.

Link zum Produkt

Dokumentation für Partner

Elastic

Integrationstyp: Empfangen

Elasticentwickelt suchgestützte Lösungen für Sicherheit, Beobachtbarkeit und Suche. Mit der Security Hub CSPM-Integration werden Ergebnisse und Erkenntnisse aus Security Hub CSPM programmatisch Elastic aufgenommen, für Korrelation und Analyse normalisiert und einheitliche Dashboards und Erkennungen angezeigt, sodass eine schnellere Auswahl und Untersuchung ohne Einsatz von Agenten ermöglicht wird. Elastic Security

Link zum Produkt

Dokumentation für Partner

Fortinet – Für TICNP

Integrationstyp: Empfangen

FortiCNPist ein Cloud-Native-Protection-Produkt, das Sicherheitserkenntnisse zu umsetzbaren Erkenntnissen zusammenfasst und Sicherheitsinformationen auf der Grundlage der Risikobewertung priorisiert, um Alarmermüdung zu reduzieren und Problembehebungen zu beschleunigen.

AWS Link zum Marketplace

Dokumentation für Partner

IBM – QRadar

Integrationstyp: Empfangen

IBM QRadarSIEM bietet Sicherheitsteams die Möglichkeit, Bedrohungen schnell und präzise zu erkennen, zu priorisieren, zu untersuchen und darauf zu reagieren.

Link zum Produkt

Dokumentation für Partner

Logz.io Cloud-SIEM

Integrationstyp: Empfangen

Logz.ioist ein AnbieterCloud SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten bereitstellt, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren.

Link zum Produkt

Dokumentation für Partner

MetricStream – CyberGRC

Integrationstyp: Empfangen

MetricStream CyberGRChilft Ihnen bei der Verwaltung, Messung und Minderung von Cybersicherheitsrisiken. Durch den Erhalt der CSPM-Ergebnisse von Security Hub erhalten Sie CyberGRC einen besseren Einblick in diese Risiken, sodass Sie Investitionen in Cybersicherheit priorisieren und IT-Richtlinien einhalten können.

AWS Link zum Marketplace

Link zum Produkt

MicroFocus – MicroFocus Arcsight

Integrationstyp: Empfangen

ArcSightbeschleunigt die effektive Erkennung und Reaktion auf Bedrohungen in Echtzeit und integriert dabei die Korrelation von Ereignissen sowie überwachte und unbeaufsichtigte Analysen mit der Automatisierung und Orchestrierung von Reaktionen.

Link zum Produkt

Dokumentation für Partner

Schwachstellenmanagement von New Relic

Integrationstyp: Empfangen

New Relic Vulnerability Managementempfängt Sicherheitsergebnisse von Security Hub CSPM, sodass Sie einen zentralen Überblick über die Sicherheit und die Leistungstelemetrie im Kontext Ihres gesamten Stacks erhalten.

AWS Link zum Marketplace

Dokumentation für Partner

PagerDuty – PagerDuty

Integrationstyp: Empfangen

Die PagerDuty digitale Betriebsmanagement-Plattform ermöglicht es Teams, proaktiv Probleme zu lösen, die sich auf Kunden auswirken, indem jedes Signal automatisch in die richtigen Erkenntnisse und Maßnahmen umgewandelt wird.

AWS Benutzer können die PagerDuty Reihe von AWS Integrationen nutzen, um ihre AWS und hybride Umgebungen vertrauensvoll zu skalieren.

In Verbindung mit den aggregierten und organisierten Sicherheitswarnungen von Security Hub CSPM PagerDuty können Teams ihren Prozess zur Reaktion auf Bedrohungen automatisieren und schnell benutzerdefinierte Aktionen einrichten, um potenziellen Problemen vorzubeugen.

PagerDutyBenutzer, die ein Cloud-Migrationsprojekt durchführen, können schnell handeln und gleichzeitig die Auswirkungen von Problemen verringern, die während des Migrationszyklus auftreten.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Cortex XSOAR

Integrationstyp: Empfangen

Cortex XSOARist eine SOAR-Plattform (Security Orchestration, Automation and Response), die sich in Ihr gesamtes Sicherheitsprodukteportfolio integrieren lässt, um die Reaktion auf Vorfälle und die Sicherheitsabläufe zu beschleunigen.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – VM-Series

Integrationstyp: Empfangen

Palo Alto VM-SeriesDie Integration mit Security Hub CSPM sammelt Bedrohungsinformationen und sendet sie als automatische Aktualisierung der Sicherheitsrichtlinien an die Firewall der VM-Series nächsten Generation, die böswillige IP-Adressaktivitäten blockiert.

Link zum Produkt

Dokumentation für Partner

Rackspace-Technologie – Cloud Native Security

Art der Integration: Empfangen

Rackspace Technology bietet zusätzlich zu systemeigenen Sicherheitsprodukten verwaltete AWS Sicherheitsdienste für die Überwachung rund um die Uhr durch Rackspace SOC, erweiterte Analysen und die Beseitigung von Bedrohungen.

Link zum Produkt

Rapid7 – InsightConnect

Integrationstyp: Empfangen

Rapid7 InsightConnectist eine Lösung zur Sicherheitsorchestrierung und Automatisierung, mit der Ihr Team den SOC-Betrieb mit wenig bis gar keinem Code optimieren kann.

Link zum Produkt

Dokumentation für Partner

RSA – RSA Archer

Integrationstyp: Empfangen

RSA ArcherMit IT- und Sicherheitsrisikomanagement können Sie ermitteln, welche Ressourcen für Ihr Unternehmen von entscheidender Bedeutung sind, Sicherheitsrichtlinien und -standards festlegen und kommunizieren, Angriffe erkennen und darauf reagieren, Sicherheitsmängel identifizieren und beheben sowie klare Best Practices für das IT-Risikomanagement festlegen.

Link zum Produkt

Dokumentation für Partner

ServiceNow – ITSM

Integrationstyp: Empfangen und aktualisieren

ServiceNowDurch die Integration mit Security Hub CSPM können die Sicherheitsergebnisse von Security Hub CSPM darin eingesehen werden. ServiceNow ITSM Sie können auch so konfigurierenServiceNow, dass automatisch ein Vorfall oder ein Problem erstellt wird, wenn es ein Ergebnis von Security Hub CSPM erhält.

Alle Aktualisierungen dieser Vorfälle und Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub CSPM.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video AWS Security Hub CSPM — Bidirektionale Integration mit. ServiceNow ITSM

Link zum Produkt

Dokumentation für Partner

Slack – Slack

Integrationstyp: Empfangen

Slackist eine Ebene des Technologie-Stacks für Unternehmen, die Menschen, Daten und Anwendungen zusammenbringt. Es ist ein zentraler Ort, an dem Menschen effektiv zusammenarbeiten, wichtige Informationen finden und auf Hunderttausende kritischer Anwendungen und Services zugreifen können, um Spitzenleistungen zu erbringen.

Link zum Produkt

Dokumentation für Partner

Splunk – Splunk Enterprise

Integrationstyp: Empfangen

Splunkverwendet Amazon CloudWatch Events als Nutzer von Security Hub CSPM-Ergebnissen. Senden Sie Ihre Daten Splunk für erweiterte Sicherheitsanalysen und SIEM an.

Link zum Produkt

Dokumentation für Partner

Splunk – Splunk Phantom

Integrationstyp: Empfangen

Mit der Splunk Phantom Anwendung für AWS Security Hub CSPM werden die Ergebnisse Phantom zur automatisierten Kontextanreicherung mit zusätzlichen Bedrohungsinformationen oder zur Durchführung automatisierter Reaktionsmaßnahmen gesendet.

Link zum Produkt

Dokumentation für Partner

ThreatModeler

Integrationstyp: Empfangen

ThreatModelerist eine automatisierte Lösung zur Bedrohungsmodellierung, die den Lebenszyklus von Unternehmenssoftware und Cloud-Entwicklung schützt und skaliert.

Link zum Produkt

Dokumentation für Partner

Trellix – Trellix Helix

Integrationstyp: Empfangen

Trellix Helixist eine in der Cloud gehostete Plattform für Sicherheitsoperationen, die es Unternehmen ermöglicht, die Kontrolle über jeden Vorfall von der Warnung bis zur Behebung zu übernehmen.

Link zum Produkt

Dokumentation für Partner

Third-party Integrationen, die Ergebnisse an Security Hub CSPM senden und Ergebnisse von Security Hub empfangen

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse an Security Hub CSPM senden und Ergebnisse von Security Hub CSPM empfangen.

Caveonix – Caveonix Cloud

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Die Caveonix AI-powered Plattform automatisiert Transparenz, Bewertung und Risikominderung in Hybrid-Clouds und deckt Cloud-native Dienste, VMs und Container ab. Integriert in AWS Security Hub CSPM, Caveonix führt AWS Daten und erweiterte Analysen zusammen, um Einblicke in Sicherheitswarnungen und Compliance zu erhalten.

AWS Link zum Marketplace

Dokumentation für Partner

Cloud Custodian – Cloud Custodian

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianermöglicht es Benutzern, in der Cloud gut verwaltet zu werden. Das einfache YAML-DSL ermöglicht einfach zu definierende Regeln, um eine gut verwaltete Cloud-Infrastruktur zu ermöglichen, die sowohl sicher als auch kostenoptimiert ist.

Link zum Produkt

Dokumentation für Partner

DisruptOps, Inc. – DisruptOPS

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Die DisruptOps Security Operations Platform unterstützt Unternehmen dabei, mithilfe automatisierter Leitplanken die besten Sicherheitspraktiken in Ihrer Cloud aufrechtzuerhalten.

Link zum Produkt

Dokumentation für Partner

Kion

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(ehemals cloudtamer.io) ist eine komplette Cloud-Governance-Lösung für. AWSKionbietet Stakeholdern Einblick in den Cloud-Betrieb und hilft Cloud-Nutzern dabei, Konten zu verwalten, Budget und Kosten zu kontrollieren und die kontinuierliche Einhaltung von Vorschriften sicherzustellen.

Link zum Produkt

Dokumentation für Partner

Turbot – Turbot

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotstellt sicher, dass Ihre Cloud-Infrastruktur sicher, konform, skalierbar und kostenoptimiert ist.

Link zum Produkt

Dokumentation für Partner

Integration von Security Hub CSPM mit kundenspezifischen Produkten

Zusätzlich zu den Ergebnissen, die durch integrierte AWS Dienste und Produkte von Drittanbietern generiert wurden, kann AWS Security Hub CSPM auch Erkenntnisse nutzen, die von anderen kundenspezifischen Sicherheitsprodukten generiert wurden.

Sie können diese Ergebnisse mithilfe der Security Hub CSPM-API an BatchImportFindingsSecurity Hub CSPM senden. Sie können denselben Vorgang verwenden, um Ergebnisse von benutzerdefinierten Produkten zu aktualisieren, die Sie bereits an Security Hub CSPM gesendet haben.

Verwenden Sie bei der Einrichtung der benutzerdefinierten Integration die Richtlinien und Checklisten im Security Hub CSPM Partner Integration Guide.

Anforderungen und Empfehlungen für kundenspezifische Produktintegrationen

Bevor Sie den `BatchImportFindings`API-Vorgang erfolgreich aufrufen können, müssen Sie Security Hub CSPM aktivieren.

Sie müssen außerdem mithilfe von Suchdetails für das benutzerdefinierte Produkt angeben. the section called “Suchformat: ASFF” Lesen Sie sich die folgenden Anforderungen und Empfehlungen für kundenspezifische Produktintegrationen durch:

Einstellen des Produkt-ARNs

Wenn Sie Security Hub CSPM aktivieren, wird ein Standardprodukt Amazon Resource Name (ARN) für Security Hub CSPM in Ihrem aktuellen Konto generiert.

Dieser Produkt-ARN weist das folgende Format auf: `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Beispiel, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Verwenden Sie diesen Produkt-ARN als Wert für das `ProductArn`-Attribut, wenn Sie die `BatchImportFindings`-API-Operation aufrufen.

Festlegung der Firmen- und Produktnamen

Sie können `BatchImportFindings` damit einen bevorzugten Firmen- und Produktnamen für die benutzerdefinierte Integration festlegen, die Ergebnisse an Security Hub CSPM sendet.

Ihre angegebenen Namen ersetzen den vorkonfigurierten Firmennamen und den Produktnamen, genannt persönlicher Name bzw. Standardname, und werden in der Security Hub CSPM-Konsole und in der JSON jedes Ergebnisses angezeigt. Siehe BatchImportFindings um Anbieter zu finden.

Einstellen der Ergebnis-IDs

Sie müssen Ihre eigenen Ergebnis-IDs mit dem `Id`-Attribut bereitstellen, verwalten und inkrementieren.

Jeder neue Befund sollte eine eindeutige Ergebnis-ID haben. Wenn das benutzerdefinierte Produkt mehrere Ergebnisse mit derselben Befund-ID sendet, verarbeitet Security Hub CSPM nur den ersten Befund.

Einstellen der Konto-ID

Sie müssen mit dem `AwsAccountId`-Attribut Ihre eigene Konto-ID angeben.

Einstellen Erstellungs- und Aktualisierungsdatums

Sie müssen eigene Zeitstempel für die Attribute `CreatedAt` und `UpdatedAt` angeben.

Importieren von Ergebnissen aus benutzerdefinierten Produkten

Zusätzlich zum Senden neuer Ergebnisse aus benutzerdefinierten Produkten können Sie auch die `BatchImportFindings`-API-Operation verwenden, um vorhandene Ergebnisse aus benutzerdefinierten Produkten zu aktualisieren.

Um vorhandene Ergebnisse zu aktualisieren, verwenden Sie die vorhandene Ergebnis-ID (über das `Id`-Attribut). Senden Sie das vollständige Ergebnis erneut mit den entsprechenden Informationen, die in der Anforderung aktualisiert wurden, einschließlich eines geänderten `UpdatedAt`-Zeitstempels.

Beispiel für benutzerdefinierte Integrationen

Sie können das folgende Beispiel für benutzerdefinierte Produktintegrationen als Leitfaden verwenden, um Ihre eigenen maßgeschneiderten Lösungen zu erstellen:

Ergebnisse von Chef InSpec Scans an Security Hub CSPM senden

Sie können eine CloudFormation Vorlage erstellen, die einen Chef InSpec Konformitätsscan durchführt und die Ergebnisse dann an Security Hub CSPM sendet.

Weitere Informationen finden Sie unter Kontinuierliche Compliance-Überwachung mit Chef InSpec und AWS Security Hub CSPM.

Von entdeckte Container-Schwachstellen Trivy an Security Hub CSPM senden

Sie können eine CloudFormation Vorlage erstellen, mit der Container AquaSecurity Trivy nach Sicherheitslücken gescannt werden, und die gefundenen Sicherheitslücken dann an Security Hub CSPM gesendet werden.

Weitere Informationen finden Sie unter So erstellen Sie eine CI/CD Pipeline für Container-Schwachstellenscans mit Trivy und AWS Security Hub CSPM.

Integration von Security Hub CSPM mit Microsoft Azure

Um Ihre Microsoft Azure-Ressourcen zu überwachen, können Sie Microsoft Azure in AWS Security Hub CSPM integrieren. Security Hub CSPM aktiviert dann automatisch Posture Management-Checks für Ihre Azure-Umgebung und generiert Erkenntnisse über Ihre Umgebung. Genauer gesagt bietet Ihnen der Dienst Folgendes:

> **Note**
>
> Sie können Azure-Standards und -Steuerungen mithilfe der Security Hub CSPM-Konsole, APIs und verwalten. AWS CloudFormation Die zentrale CSPM-Konfigurationsfunktion von Security Hub wird für Azure-Standards nicht unterstützt.

- ASFF-Ergebnisse — Security Hub CSPM generiert Ergebnisse im AWS Security Finding Format (ASFF) -Format für Statusprüfungen, die es für Ihre Azure-Ressourcen durchführt.
- CIS Microsoft Azure Foundations Benchmark v4.0 — Automatisierte Konformitätsprüfungen anhand des CIS Azure v4.0-Standards. Dieser Standard umfasst Identitäts-, Netzwerk-, Speicher-, Protokollierungs- und Datenbankkontrollen.
- Azure Foundational Best Practices — Automatisierte Erkennung von Fehlkonfigurationen von Azure-Ressourcen auf der Grundlage von AWS kuratierten bewährten Sicherheitsmethoden in den Bereichen Netzwerksicherheit, Identitätsmanagement, Datenschutz und Protokollierung.
- Posture Management — Kontinuierliche Bewertung der Azure-Ressourcenkonfigurationen anhand von bewährten Sicherheitsmethoden und Compliance-Standards mit 122 Kontrollen für beide Standards.
- Per-provider Sicherheitsbewertungen — Separate Sicherheitsbewertungen für AWS und Azure, sodass Sie jede Umgebung unabhängig verfolgen können.

Um die Integration zu erstellen, verbinden Sie Ihre Azure-Umgebung über den folgenden Prozess mit Security Hub CSPM:

> **Note**
>
> Azure-Standards unterscheiden sich in folgenden Punkten von AWS Standards:
>
> - Azure-Standards erfordern keine manuellen AWS Config Voraussetzungen. Anders als Kunden AWS, die einen CSPM-only vom Kunden verwalteten Rekorder benötigen, verwenden die Azure-Standards automatisch einen internen, serviceverknüpften Rekorder.
> - Azure-Standards verwenden immer interne, dienstbezogene Konfigurationsregeln. AWS Standards verwenden nur dann serviceverknüpfte Konfigurationsregeln, wenn Security Hub ebenfalls aktiviert ist.

1. Sie konfigurieren Ihre Azure-Umgebung mit einer Anwendungsregistrierung, föderierten Identitätsanmeldedaten, Azure-Rollenzuweisungen und einer Event Hub-Infrastruktur.
2. Mithilfe der Security Hub CSPM-Konsole erstellen Sie einen Connector für die Integration. Sie geben Ihre Azure-Mandanten-ID, Anwendungsclient-ID und den Überwachungsumfang an.
3. AWS Config sammelt Daten zur Ressourcenkonfiguration aus Ihrer Azure-Umgebung.

   AWS Config wird intern verwendet, um Ressourcenkonfigurationsdaten zu sammeln. Im Gegensatz zur AWS Posture Management, bei der Sie die Aufzeichnung explizit aktivieren AWS Config und dafür bezahlen müssen, erfolgt die Verarbeitung bei Azure Posture Management AWS Config automatisch. Sie müssen den Recorder nicht AWS Config separat aktivieren, konfigurieren oder separat für die AWS Config Nutzung bezahlen. Diese Kosten sind in Ihren Security Hub CSPM-Preisen enthalten.
4. Security Hub CSPM beginnt mit dem Empfang von Ressourcenkonfigurationsdaten und Aktivitätsprotokollereignissen aus Ihrer Azure-Umgebung.
5. Security Hub CSPM generiert Informationen zur Statusverwaltung über Ihre Azure-Umgebung.

Wie AWS Config wird verwendet

AWS Config wird intern verwendet, um Daten zur Ressourcenkonfiguration zu sammeln und Änderungen in Ihrer Azure-Umgebung zu erkennen. Der Connector verarbeitet dies automatisch. Sie müssen den Recorder nicht AWS Config separat aktivieren, konfigurieren oder für die AWS Config

Nutzung bezahlen. Diese Kosten sind in Ihren Security Hub CSPM-Preisen für Azure-Ressourcen enthalten.

Service-linked Konnektoren und vom Kunden verwaltete Konnektoren

Security Hub CSPM unterstützt zwei Arten von Konnektoren:

Service-linked Anschluss (SLC)

Wird automatisch erstellt, wenn Sie die Azure-Integration in Security Hub einrichten. Der Geltungsbereich eines serviceverknüpften Connectors entspricht immer dem Bereich, der in Ihrem Security Hub Hub-Connector definiert ist. Sie können den Bereich eines serviceverknüpften Connectors nicht direkt ändern. Ändern Sie stattdessen den Bereich in Security Hub. Security Hub verwaltet den Lebenszyklus von serviceverknüpften Connectors in Ihrem Namen.

Customer-managed Anschluss (CMC)

Direkt in der Security Hub CSPM-Konsole auf der Seite Integrationen erstellt. Verwenden Sie einen vom Kunden verwalteten Connector, wenn Sie Security Hub CSPM unabhängig von Security Hub verwenden möchten oder wenn Sie einen anderen Bereich als Ihren Security Hub Hub-Connector benötigen. Wenn beide Typen existieren, muss der Umfang des serviceverknüpften Connectors immer dem Umfang Ihres vom Kunden verwalteten Connectors entsprechen oder diesen überschreiten.

> **Note**
>
> Im Gegensatz zu Security Hub bietet Security Hub CSPM keine funktionsspezifische Auswahl für Azure-Konnektoren. Wenn Sie einen Connector in Security Hub CSPM erstellen, werden alle Funktionen zur Statusverwaltung zusammen aktiviert.

Informationen zur Schätzung und Berechnung der Kosten für die Integration von Security Hub CSPM mit Azure finden Sie unter AWS Security Hub CSPM-Preise.

Themen

- Voraussetzungen für die Integration von Security Hub CSPM mit Microsoft Azure
- Konfiguration von Microsoft Azure für die Integration mit Security Hub CSPM
- Konfiguration von Security Hub CSPM für die Integration mit Microsoft Azure

- Löschen eines Microsoft Azure-Connectors in Security Hub CSPM

Voraussetzungen für die Integration von Security Hub CSPM mit Microsoft Azure

Bevor Sie Microsoft Azure in AWS Security Hub CSPM integrieren, führen Sie die folgenden Aufgaben in Ihrer AWS und Ihrer Azure-Umgebung durch. Dadurch wird sichergestellt, dass Sie und Security Hub CSPM über die Ressourcen und Berechtigungen verfügen, die Sie zur Überwachung Ihrer Azure-Ressourcen benötigen.

Themen

- Voraussetzungen für AWS
- Voraussetzungen für Microsoft Azure

Voraussetzungen für AWS

Stellen Sie sicher, dass Sie Folgendes in Ihrem haben AWS-Konto:

AWS Security Hub CSPM aktiviert

Security Hub CSPM muss an der AWS-Region Stelle aktiviert sein, an der AWS-Konto Sie den Connector erstellen möchten.

IAM-Berechtigungen für die Konsole

Der IAM-Prinzipal, der den Connector erstellt, muss über die folgenden Berechtigungen verfügen:

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

IAM Outbound Identity Federation ist aktiviert

Sie müssen IAM Outbound Identity Federation in Ihrem aktivieren. AWS-Konto Diese Funktion ermöglicht es AWS Diensten, sich bei externen Identitätsanbietern (wie Microsoft Entra ID) zu authentifizieren, indem sie föderierte Anmeldeinformationen anstelle von langlebigen Geheimnissen verwenden.

Notieren Sie sich nach der Aktivierung von Outbound Identity Federation die URL des Token-Ausstellers. Diese URL folgt dem Format:

```
https://uuid.tokens.sts.global.api.aws
```

Sie benötigen diese URL, wenn Sie Anmeldeinformationen für föderierte Identitäten in Azure konfigurieren.

Voraussetzungen für Microsoft Azure

Stellen Sie sicher, dass in Ihrer Azure-Umgebung Folgendes vorhanden ist:

Azure-Mandant

Sie benötigen einen Azure-Mandanten in der kommerziellen Azure-Cloud. Azure Government und Azure China werden nicht unterstützt.

Verfügbarkeit des Microsoft Entra ID-Protokolls

Für die Ressourcenaufzeichnung sind Microsoft Graph-Auditprotokolle und Anmeldeprotokolle von Ihrem Microsoft Entra ID-Mandanten erforderlich. Für einige Microsoft Entra ID-Protokolle ist eine Microsoft Entra ID P1- oder P2-Lizenzierung erforderlich.

Wenn dem Mandanten die erforderlichen Protokolle fehlen, meldet die Ressourcenaufzeichnung möglicherweise Teilausfälle. Die App-Registrierung und die Azure-Rollenzuweisungen liefern keine fehlenden Protokolldaten.

Rolle „Globaler Administrator“

Die Person, die die Azure-Umgebung konfiguriert, muss die globale Administratorrolle in Microsoft Entra ID haben. Diese Rolle ist erforderlich, um Anwendungen zu registrieren, die Zustimmung des Administrators für Microsoft Graph-API-Berechtigungen zu erteilen, RBAC-Rollen im Bereich der Mandantenstammverwaltungsgruppe zuzuweisen und Diagnoseeinstellungen für Entra ID Audit Logs zu konfigurieren.

> **Note**
>
> In vielen Organisationen sind der globale Azure-Administrator und der AWS Sicherheitsadministrator unterschiedliche Personen. Das Azure-Setup kann mithilfe des generierten Setup-Skripts unabhängig abgeschlossen werden.

Registrierung der Azure-App

Sie müssen eine Anwendung in Microsoft Entra ID registrieren. Diese Anwendung dient als Identität, die für die Authentifizierung in Ihrer Azure-Umgebung mithilfe von Verbundanmeldedaten AWS verwendet wird. Es sind keine Client-Geheimnisse erforderlich.

Azure Event Hub

Sie müssen einen Azure Event Hub-Namespace und eine Event Hub-Instanz erstellen, um Activity Log- und Entra ID Audit Log-Ereignisse zu empfangen. Das Setup-Skript automatisiert diese Erstellung.

Microsoft Graph-API-Berechtigungen

Die registrierte Anwendung benötigt die folgenden Microsoft Graph-API-Berechtigungen (Anwendungstyp, erfordert Zustimmung des Administrators):

- `Directory.Read.All`— Lesen Sie Verzeichnisdaten, einschließlich Benutzer, Gruppen und Dienstprinzipalen.
- `AuditLog.Read.All`— Lesen Sie die Ereignisse des Entra ID-Prüfprotokolls.
- `Policy.Read.All`— Lesen Sie Unternehmensrichtlinien und Konfigurationen für bedingten Zugriff.

Rolle „Azure RBAC Reader“

Dem Dienstprinzipal muss die Rolle Reader im Bereich der Stammverwaltungsgruppe des Mandanten zugewiesen werden. Dadurch wird schreibgeschützter Zugriff auf alle Azure-Ressourcen für alle Abonnements im Mandanten gewährt.

Nachdem Sie diese Aufgaben abgeschlossen haben, können Sie Ihre Azure-Umgebung konfigurieren.

Konfiguration von Microsoft Azure für die Integration mit Security Hub CSPM

Nachdem Sie die erforderlichen Aufgaben abgeschlossen haben, können Sie Ihre Microsoft Azure-Umgebung so konfigurieren, dass die Integration mit AWS Security Hub CSPM unterstützt wird. Um Ihnen dabei zu helfen, generiert die Security Hub CSPM-Konsole ein Setup-Skript, das auf Ihre Konfiguration zugeschnitten ist.

Gehen Sie wie folgt vor, um das Skript zu generieren:

1. Öffnen Sie die Security Hub CSPM-Konsole.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie Azure-Connector erstellen.
4. Vervollständigen Sie die Connector-Konfiguration (Mandanten-ID, Bereich und Name) und kopieren Sie dann das generierte Setup-Skript.

Um das Skript auszuführen, verwenden Sie die Azure-CLI und authentifizieren Sie sich mit einem globalen Administratorkonto (`az login`).

Wenn Sie das Skript ausführen, führt es eine Reihe von Aufgaben aus. In den folgenden Abschnitten wird jede Aufgabe beschrieben, die das Skript ausführt. Wenn Ihre Organisation die Ausführung von Skripten einschränkt, können Sie diese Aufgaben manuell ausführen, indem Sie dieses Thema als Leitfaden verwenden. Nachdem Sie Ihre Azure-Umgebung konfiguriert haben, können Sie Security Hub CSPM für die Integration in Azure konfigurieren.

> **Note**
>
> Eine einzige Azure-App-Registrierung wird von allen AWS Sicherheitsdiensten gemeinsam genutzt. Wenn Sie auch Security Hub oder Amazon Inspector for Azure verwenden, verwenden diese dieselbe App-Registrierung. Sie müssen nicht für jeden AWS Dienst separate Registrierungen erstellen.

Aufgaben

- Schritt 1: Registrieren Sie eine Azure-Anwendung
- Schritt 2: Erstellen Sie einen Service Principal
- Schritt 3: Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität
- Schritt 4: Weisen Sie die Leser-Rolle zu
- Schritt 5: Konfigurieren Sie die Microsoft Graph API-Berechtigungen
- Schritt 6: Azure Event Hub einrichten
- Schritt 7: Konfigurieren Sie das Aktivitätsprotokoll und den Export des Entra ID-Auditprotokolls

Schritt 1: Registrieren Sie eine Azure-Anwendung

Registrieren Sie eine neue Anwendung in Microsoft Entra ID. Diese Anwendung dient als Identität, die zur Authentifizierung in Ihrer Azure-Umgebung mithilfe von Verbundanmeldeinformationen AWS verwendet wird. Es sind keine Client-Geheimnisse erforderlich.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Notieren Sie sich die Anwendungs-ID (Client) aus der Ausgabe (das `appId` Attribut). Sie geben diesen Wert an, wenn Sie den Connector in der Security Hub CSPM-Konsole erstellen.

Schritt 2: Erstellen Sie einen Service Principal

Erstellen Sie einen Dienstprinzipal für die registrierte Anwendung. Sie verwenden Azure-Rollenzuweisungen, um dem Dienstprinzipal Berechtigungen zu erteilen. Der Dienstprinzipal führt Aktionen in Ihrer Azure-Umgebung durch.

```
$ az ad sp create --id application-client-id
```

Wo *`application-client-id`* ist die Anwendungs-ID (Client) aus dem vorherigen Schritt.

Schritt 3: Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität

Konfigurieren Sie die Anmeldeinformationen für die Verbundidentität in der Anwendung, um eine Authentifizierung ohne AWS geheime Client-Schlüssel zu ermöglichen. Dadurch wird eine OIDC-Vertrauensstellung zwischen und Azure hergestellt. AWS Es werden keine langlebigen Geheimnisse oder Anmeldeinformationen gespeichert.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "AWSConfigFederation",
    "issuer": "token-issuer-url",
    "subject": "arn:aws:iam::account-id:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "Federation for AWS Config third-party cloud resource discovery"
  }'
```

Die wichtigsten Werte:

- Aussteller — Ihre Token-Aussteller-URL von IAM Outbound Identity Federation. Dies folgt dem Format. `https://uuid.tokens.sts.global.api.aws`
- Betreff — Der ARN der `AWSServiceRoleForConfigThirdParty` dienstverknüpften Rolle in Ihrem AWS-Konto. AWS erstellt diese serviceverknüpfte Rolle automatisch während der Connector-Setup.
- Zielgruppe — `api://AzureADTokenExchange` (Standardwert für den Workload-Identitätsverbund).

Schritt 4: Weisen Sie die Leser-Rolle zu

Weisen Sie dem Dienstprinzipal im Stammbereich (/) die Leserrolle zu. Dadurch wird Lesezugriff auf alle Azure-Ressourcen für alle Abonnements im Mandanten gewährt.

Weisen Sie Reader im Root-Bereich zu

Stellen Sie sicher, dass Sie die Reader-Rolle im Stammbereich (/) zuweisen, nicht im Bereich der Mandanten-Stammverwaltungsgruppe. Security Hub CSPM liest Azure-Ressourcen für die Rollenzuweisung in jedem Bereich, einschließlich Zuweisungen, die sich auf den Mandantenstamm beziehen. Eine Leserzuweisung in der Stammverwaltungsgruppe deckt keine Aufgaben ab/, deren Geltungsbereich darin liegt. Andernfalls schlagen diese Lesevorgänge mit einem Autorisierungsfehler fehl und der Connector kann in einen herabgesetzten Zustand übergehen.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope Für eine Zuweisung sind erweiterte Zugriffsrechte erforderlich

Für die Zuweisung einer Rolle im Stammbereich (/) sind erhöhte Zugriffsrechte erforderlich. Wenn eine Rollenzuweisung fehlschlägt, stellen Sie sicher, dass die Zugriffsverwaltung für Azure-Ressourcen unter Microsoft Entra ID > Eigenschaften auf Ja gesetzt ist. Melden Sie sich dann ab und wieder an, um Ihr Token zu aktualisieren.

⚠ Entfernen Sie die temporäre Wurzelhöhe

Wenn Sie die Zugriffsverwaltung für Azure-Ressourcen aktivieren, wird dem angemeldeten Administrator die Rolle des Benutzerzugriffsadministrators im Stammbereich (/) zugewiesen, der den Zugriff für jedes Abonnement und jede Verwaltungsgruppe im Mandanten verwalten kann. Wenn das Onboarding abgeschlossen ist, setzen Sie die Zugriffsverwaltung für Azure-Ressourcen unter Microsoft Entra ID > Eigenschaften wieder auf Nein, speichern Sie und melden Sie sich ab, damit diese Erhöhung nicht aktiv bleibt.

Schritt 5: Konfigurieren Sie die Microsoft Graph API-Berechtigungen

Erteilen Sie der Anwendung die folgenden Microsoft Graph API-Berechtigungen (Anwendungstyp) und erteilen Sie dann die Zustimmung des Administrators:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Schritt 6: Azure Event Hub einrichten

AWS Config verwendet einen Azure Event Hub, um nahezu in Echtzeit Benachrichtigungen über Änderungen der Ressourcenkonfiguration in Ihrer Azure-Umgebung zu erhalten. Das Setup-Skript erstellt die Event Hub-Infrastruktur und markiert sie zur Erkennung.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 1 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Nachdem Sie den Event Hub erstellt haben, kennzeichnen Sie den Namespace für die Erkennung und weisen Sie die Rolle des Datenempfängers zu:

```
$ az tag create \
  --resource-id namespace-resource-id \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> Im Tag-Format *account-id* ist AWSConfig-*account-id*-*region* dies Ihre 12-stellige AWS-Konto ID und *region* der Ort, AWS-Region an dem Sie den Connector erstellen (z.

B.`us-east-1`). Diese Werte geben an, welcher AWS-Konto und welcher Region diese Event Hub-Integration gehört.

Wichtige Konfiguration:

- Namespace-SKU — Standard (für Verbrauchergruppen erforderlich).
- Name des Event Hubs —`activitylog`.
- Verbrauchergruppe —`AWSConfig`.
- Tag — `AWSConfig-`*`account-id`*`-`*`region`* mit Wert`activitylog`. Dieses Tag ermöglicht es AWS Config , den Event Hub automatisch zu erkennen.
- Rollenzuweisung — Azure Event Hubs Data Receiver im Namespace.

Schritt 7: Konfigurieren Sie das Aktivitätsprotokoll und den Export des Entra ID-Auditprotokolls

Konfigurieren Sie Azure so, dass Aktivitätsprotokolle und Entra ID-Auditprotokolle in den Event Hub exportiert werden.

Export des Aktivitätsprotokolls:

Konfigurieren Sie die Diagnoseeinstellungen für jedes Abonnement, um Aktivitätsprotokolle in den Event Hub zu exportieren. Das Setup-Skript konfiguriert dies automatisch für alle überwachten Abonnements. Aktivitätsprotokolle erfassen Aktivitäten auf Abonnementebene, einschließlich Rollenzuweisungen und Ressourcenänderungen.

Export des Entra ID-Auditprotokolls:

Konfigurieren Sie die Diagnoseeinstellungen auf der Microsoft Entra ID, um Auditprotokolle in denselben Event Hub zu exportieren. Navigieren Sie zu Microsoft Entra ID > Überwachung > Diagnoseeinstellungen > Diagnoseeinstellung hinzufügen. Aktiviere sie AuditLogs und leite sie an deinen Event Hub weiter.

Kontinuierlicher Export von Microsoft Defender for Cloud (optional):

Um Defender for Cloud-Sicherheitswarnungen an Security Hub CSPM weiterzuleiten, konfigurieren Sie den kontinuierlichen Export zu Ihrem Event Hub. Navigieren Sie im Azure-Portal zu Microsoft

Defender for Cloud > Umgebungseinstellungen > Wählen Sie Abonnement > Kontinuierlicher Export aus. Wählen Sie Event Hub als Exportziel und wählen Sie Ihren Event Hub-Namespace aus. Aktivieren Sie Sicherheitswarnungen als Exportdatentyp.

Konfiguration von Amazon Inspector-Datenereignissen (optional):

Wenn Sie Amazon Inspector für das Scannen von Azure-VMs verwenden möchten, ist eine zusätzliche Konfiguration für Datenereignisse erforderlich. Einzelheiten zur Konfiguration von Inspector-specific Datenereignissen finden Sie in der Amazon Inspector-Dokumentation zur Azure-Integration.

Konfiguration von Security Hub CSPM für die Integration mit Microsoft Azure

Nachdem Sie die erforderlichen Aufgaben abgeschlossen und Ihre Microsoft Azure-Umgebung konfiguriert haben, können Sie AWS Security Hub CSPM für die Integration mit Azure konfigurieren. Um Security Hub CSPM für die Integration mit Azure zu konfigurieren, erstellen Sie einen Connector. Nachdem Sie den Connector erstellt haben, treten die folgenden Ereignisse auf:

1. Security Hub CSPM validiert die Azure-Anmeldeinformationen und die Konnektivität zu Ihrer Azure-Umgebung. Dieser Vorgang kann einige Minuten dauern.
2. AWS Config beginnt mit der Erkennung und Aufzeichnung von Konfigurationsdaten für Ihre Azure-Ressourcen.
3. Security Hub CSPM beginnt nach Abschluss der Ressourcendatenerfassung mit der Generierung von Ergebnissen zur Statusverwaltung für Ihre Azure-Ressourcen.

> **Note**
>
> Wenn Sie bereits einen Connector in Security Hub erstellt haben, wurde in Security Hub CSPM automatisch ein serviceverknüpfter Connector erstellt. Sie müssen keinen separaten, vom Kunden verwalteten Connector erstellen, es sei denn, Sie benötigen einen anderen Bereich.

Themen

- Erstellen Sie einen Azure-Connector
- Aktivierung von Standards und Kontrollen

- Passen Sie den Umfang eines Azure-Connectors an
- Überprüfen Sie den Zustand eines Azure-Connectors
- Problembehandlung bei einem Azure-Connector
- Wie Security Hub CSPM mit Ressourcen-Identifikatoren umgeht
- Verfügbare Steuerelemente für Azure

Erstellen Sie einen Azure-Connector

Um einen Microsoft Azure-Connector für Ihre Umgebung zu erstellen, führen Sie die folgenden Schritte mithilfe der AWS Security Hub CSPM-Konsole oder der API aus.

1. Öffnen Sie die Security Hub CSPM-Konsole.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie Azure-Connector erstellen aus.
4. Geben Sie für Azure Tenant ID Ihre Azure Active Directory-Mandanten-ID ein.
5. Geben Sie für Anwendung (Client-ID) die Anwendungs-ID für die Azure-App-Registrierung ein, die Sie erstellt haben.
6. Konfigurieren Sie zusätzliche Einstellungen und den Umfang des Connectors, indem Sie wie folgt vorgehen:

   - Geben Sie unter Name einen eindeutigen Namen für den Connector ein. Der Name kann bis zu 50 alphanumerische Zeichen und Bindestriche (-) enthalten.

     > **Important**
     >
     > Namen und Beschreibungen werden verwendet, um Ihre Inhalte zu identifizieren. Wir empfehlen Ihnen, keine sensiblen, vertraulichen oder persönlich identifizierbaren Informationen (PII) darin zu verwenden.

   - Geben Sie unter Beschreibung optional eine kurze Beschreibung des Connectors ein. Die Beschreibung kann bis zu 200 Zeichen enthalten.
   - Wählen Sie für Abonnements Alle Abonnements aus, um alle aktuellen und future Abonnements im Mandanten zu überwachen, oder Spezifische Abonnements, um nur die von Ihnen angegebenen Abonnements zu überwachen. Wenn Sie nur bestimmte Abonnements überwachen möchten, geben Sie die ID für jedes Abonnement ein.

- Wählen Sie für Regionen die Azure-Regionen aus, in denen Ihre Ressourcen bereitgestellt werden.

> **Note**
>
> Für Kontrollen, die Microsoft Entra ID- und Microsoft Graph-Ressourcen auswerten, muss der Geltungsbereich der globalen Region in Ihrer Integrationskonfiguration enthalten sein. Wenn Sie nur bestimmte Azure-Regionen auswählen, führen diese Kontrollen nicht zu Ergebnissen.

7. Überprüfen Sie Ihre Konfiguration und wählen Sie Connector erstellen aus.

Nachdem Sie den Connector erstellt haben, validiert Security Hub CSPM Ihre Azure-Anmeldeinformationen und beginnt mit der Ressourcenerkennung. Der Connector sollte innerhalb von 2 bis 5 Minuten den Status Aktiv anzeigen.

Aktivierung von Standards und Kontrollen

Nachdem Sie den Connector erstellt haben, müssen Sie die Azure-Sicherheitsstandards aktivieren, um mit der Generierung von Ergebnissen beginnen zu können. Allgemeine Informationen zur Aktivierung von Standards und zur Verwaltung von Kontrollen finden Sie unter Aktivieren von Standards und Aktivieren und Deaktivieren von Kontrollen.

Verfügbare Standards

- CIS Microsoft Azure Foundations Benchmark v4.0 — Ein weit verbreiteter Sicherheitsbenchmark, der bewährte Methoden für die Sicherung von Azure-Umgebungen definiert. Jedes Steuerelement bewertet einen bestimmten Aspekt Ihrer Azure-Konfiguration (z. B. Verschlüsselung von Speicherkonten, Regeln für Netzwerksicherheitsgruppen, Identitäts- und Zugriffseinstellungen).
- Azure Foundational Best Practices — Evaluiert Azure-Ressourcen im Hinblick auf Expositionsrisiken, indem Indikatoren für Netzwerkerreichbarkeit, öffentlichen Zugriff und sensible Daten miteinander korreliert werden. Generiert Ergebnisse vom Typ der Exposition, anhand derer Ressourcen mit erhöhtem Risiko hervorgehoben werden.

Azure-Standards verfügen über eigene Kontrollen, die von den Kontrollen getrennt sind. AWS Es gibt keine cloudübergreifenden Kontrollen, mit denen AWS sowohl Azure-Ressourcen als auch Azure-Ressourcen in einem einzigen Check bewertet werden.

Aktivierung eines Standards

Sie können Azure-Standards über die Security Hub CSPM-Konsole oder über die aktivieren. API/CLI Navigieren Sie in der Security Hub CSPM-Konsole zu Standards und aktivieren Sie den gewünschten Standard. Verwenden Sie alternativ die CLI:

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
  --region your-aws-region
```

> **Note**
>
> Sie können Azure-Standards vor oder nach der Erstellung des Connectors aktivieren — sie sind nicht gekoppelt. Ergebnisse werden jedoch erst generiert, wenn sowohl der Konnektor als auch der Standard aktiv sind und Ressourcendaten gesammelt wurden.

Verwaltung einzelner Kontrollen

Sobald ein Standard aktiviert ist (normalerweise innerhalb von Sekunden), können Sie einzelne Steuerelemente anzeigen und verwalten:

- Steuerelemente anzeigen: Verwenden Sie die Security Hub CSPM-Konsole (Standards > Standard auswählen > Kontrollen) oder die `list-standards-control-associations` API.
- Ein Steuerelement deaktivieren: Wenn ein bestimmtes Steuerelement für Ihre Umgebung nicht gilt, können Sie es deaktivieren.
- Benutzerdefinierte Parameter konfigurieren: Einige Steuerelemente akzeptieren benutzerdefinierte Eingabeparameter (z. B. Schwellenwerte für die Kennwortlänge). Diese können über die `update-security-control` API konfiguriert werden.

Wichtige Hinweise

- Die Azure-Standards gelten einheitlich für Ihren gesamten Konnektorbereich. Sie können innerhalb desselben Connectors nicht unterschiedliche Standards oder Kontrollen für verschiedene Azure-Abonnements aktivieren.
- Die Kontrollen hängen von der Verfügbarkeit der Ressourcendaten ab. Jedes Steuerelement bewertet einen bestimmten Azure-Ressourcentyp. Wenn AWS Config noch keine Konfigurationsdaten für einen bestimmten Ressourcentyp erfasst wurden, generiert das

Steuerelement einen PASS-Standardwert für diese Ressourcen. Diese PASS-Standardergebnisse werden automatisch aktualisiert, sodass sie korrekt sind, sobald die Ressourcendaten eintreffen. Behandeln Sie die anfänglichen Compliance-Ergebnisse erst dann als korrekt, wenn die Erfassung der Ressourcendaten abgeschlossen ist.

- Benutzerdefinierte Eingabeparameter für Sicherheitskontrollen können bereits vor der Erstellung eines Connectors konfiguriert werden — sie bleiben unabhängig voneinander bestehen.
- Steuerelemente, die Einstellungen auf Abonnementebene auswerten (z. B. Microsoft Defender-Pläne, Aktivitätsprotokollwarnungen), führen zu einem Ergebnis pro Azure-Abonnement und nicht pro einzelner Ressource.
- Multicloud-Standards können nicht in die Richtlinien für die zentrale Konfiguration aufgenommen werden. Sie müssen die Azure-Standardaktivierung in beiden Bereichen unabhängig voneinander verwalten. AWS-Konto AWS-Region

Passen Sie den Umfang eines Azure-Connectors an

Nachdem Sie einen Microsoft Azure-Connector erstellt haben, können Sie den Umfang des Connectors anpassen, indem Sie die Azure-Abonnements oder Azure-Regionen ändern, die er überwacht. Wenn Sie den Umfang anpassen, werden die meisten Änderungen innerhalb von etwa 15 Minuten wirksam.

Bevor Sie den Umfang anpassen, sollten Sie Folgendes beachten:

- Der Umfang eines vom Kunden verwalteten Connectors darf den Umfang eines vorhandenen serviceverknüpften Connectors in demselben Konto und derselben Region nicht überschreiten.
- Wenn Sie den Umfang erweitern, beginnt Security Hub CSPM, Ergebnisse für neue Ressourcen zu generieren, nachdem deren AWS Config Konfigurationsdaten erfasst wurden.
- Wenn Sie den Umfang reduzieren, werden die vorhandenen Ergebnisse für entfernte Ressourcen in den Status „Archiviert“ überführt.

Überprüfen Sie den Zustand eines Azure-Connectors

Sie können den Zustand eines Microsoft Azure-Connectors jederzeit überprüfen. Navigieren Sie in der Security Hub CSPM-Konsole zu Integrationen und vergewissern Sie sich, dass Ihr Connector den Status Aktiv anzeigt.

Erste Ergebnisse werden in der Regel innerhalb von 15 bis 30 Minuten nach Abschluss der Erfassung der Ressourcendaten sichtbar.

> **Note**
>
> Der Integritätsstatus des Connectors ist letztendlich konsistent. Wenn ein Berechtigungs- oder Konfigurationsproblem auftritt, ändert sich der Status des Connectors schnell in Heruntergestuft und es wird eine umsetzbare Meldung angezeigt. Nachdem Sie das Problem behoben haben, kann es jedoch bis zu 24 Stunden dauern, bis der Status wieder zu Verbunden zurückkehrt.
>
> - Ein Status „Heruntergestuft“ nach einem kürzlich erfolgten Update weist nicht unbedingt auf ein anhaltendes Problem hin.
> - Überprüfen Sie die CloudWatch Metriken im Namespace, um in Echtzeit Einblick in die Fehler bei der Aufzeichnung zu erhalten.

Problembehandlung bei einem Azure-Connector

Wenn Sie Probleme mit Ihrem Connector haben, verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben.

Der Status des Connectors ist fehlerhaft

Dieses Problem tritt normalerweise auf, wenn Verbundanmeldeinformationen in Azure nicht korrekt konfiguriert sind.

Um dieses Problem zu beheben, stellen Sie sicher, dass die URL des Token-Ausstellers und der Betreff-ARN in Ihren Azure-Verbundanmeldedaten mit Ihren übereinstimmen. AWS-Konto

Keine Ergebnisse nach 30 Minuten

Dieses Problem kann auftreten, wenn Event Hub keine Aktivitätsprotokolle empfängt oder wenn kein Standard aktiviert ist.

Um dieses Problem zu beheben, stellen Sie sicher, dass der Event Hub-Namespace korrekt gekennzeichnet ist (`AWSConfig-`*`account-id`*`-`*`region`*`=activitylog`), dass `AWSConfig` die Nutzergruppe vorhanden ist, die Datenempfängerrolle zugewiesen ist und mindestens ein Azure-Standard aktiviert ist.

Einige Azure-Ressourcen konnten nicht aufgezeichnet werden

Der Fehler kann aus einem der folgenden Gründe auftreten:

- Die Azure-Umgebung erfüllt nicht die Voraussetzungen für die Ressourcenaufzeichnung.
- Für die App-Registrierung ist keine Administrator-Zustimmung für Microsoft Graph-API-Berechtigungen erforderlich.
- Die Rollenzuweisung Reader deckt nicht alle erforderlichen Bereiche ab.
- Der Microsoft Entra ID-Mandant verfügt nicht über die erforderlichen Protokolldaten.

Gehen Sie wie folgt vor, um den Fehler zu beheben:

1. Um zu überprüfen, ob Ihre Umgebung alle Anforderungen erfüllt, lesen Sie die Voraussetzungen für Microsoft Azure.
2. Vergewissern Sie sich mit Zustimmung des Administrators, dass die App-Registrierung über die erforderlichen Microsoft Graph-API-Berechtigungen verfügt.
3. Stellen Sie sicher, dass der Dienstprinzipal die Rolle Reader im Bereich der Stammverwaltungsgruppe des Mandanten innehat.

Der Connector bleibt im Status Ausstehend

Dieses Problem kann auftreten, wenn die Azure-App-Registrierung falsch konfiguriert ist.

Um dieses Problem zu beheben, stellen Sie sicher, dass die URL des Ausstellers der Verbundidentitätsanmeldeinformationen und die Betreff-ID mit Ihrer übereinstimmen. AWS-Konto Stellen Sie außerdem sicher, dass die Zustimmung des Administrators für alle erforderlichen Microsoft Graph-API-Berechtigungen erteilt wurde.

Wie Security Hub CSPM mit Ressourcen-Identifikatoren umgeht

Wenn Sie Ihre Azure-Integration für AWS Security Hub CSPM aktivieren, werden Ressourcen-Identifikatoren von anderen Cloud-Anbietern in AWS Config AWS Security Hub CSPM und anderen AWS Diensten (nach Bedarf) als Metadaten gespeichert, die sich auf die Verwaltung der entsprechenden Ressourcenkonfigurationsdaten beziehen, die von den anderen Cloud-Anbietern gesammelt wurden. Solche Ressourcen-Identifikatoren stellen nicht Ihre Inhalte dar, und wir empfehlen Ihnen, keine sensiblen, vertraulichen oder persönlich identifizierbaren Informationen in sie aufzunehmen.

Die folgenden Identifikatoren aus Ihrer verbundenen Cloud-Umgebung werden gespeichert und verwendet, AWS um Multi-Cloud-Sicherheitsfunktionen bereitzustellen:

- Ressourcen-IDs: Azure-Mandanten-ID, Abonnement-ID, Standort (Region), Ressourcen-ID (Ressourcengruppen-IDs oder -namen, Ressourcenanbieter, Ressourcentyp)

Beziehungen zwischen diesen Identifikatoren — einschließlich der Beziehung zwischen Ressourcen und der Beziehung der Ergebnisse zu Ressourcen — werden ebenfalls als Dienstmetadaten gespeichert. AWS verwendet diese Identifikatoren für die Korrelation von Ressourcen, für die Zuordnung von Ergebnissen zu Ressourcen, für die Protokollierung von Dienstabläufen und für die Deduplizierung.

Verfügbare Steuerelemente für Azure

Nachdem Sie die Azure-Standards aktiviert haben, bewerten die folgenden 122 Kontrollen Ihre Azure-Ressourcen. Die Kontrollen sind auf zwei Standards verteilt:

- CIS Microsoft Azure Foundations Benchmark v4.0 — 96 Kontrollen, die bestimmten CIS-Abschnitten zugeordnet sind
- Azure Foundational Best Practices — 26 Kontrollen, die zusätzliche bewährte Sicherheitsmethoden abdecken

> **Note**
>
> Für Kontrollen, die Microsoft Entra ID- und Microsoft Graph-Ressourcen auswerten, muss der Geltungsbereich der globalen Region in Ihrer Integrationskonfiguration enthalten sein.

Verfügbare Azure-Steuerelemente

Titel des Steuerelements	Ressourcentyp	Standard
Azure Container Apps mit aktivierter verwalteter Identität sollten dem Prinzip der geringsten Rechte folgen	`microsoft.app/containerapps`	Bewährte Methoden für die Grundlagen von Azure
Azure Container Apps sollten Azure SDK-Anmeldeinformationen nicht als Umgebungsvariablen übergeben	`microsoft.app/containerapps`	Bewährte Methoden für die Grundlagen von Azure
Für Azure Container Apps sollte der externe Eingang nicht aktiviert sein	`microsoft.app/containerapps`	Bewährte Methoden für die Grundlagen von Azure

Titel des Steuerelements	Ressourcentyp	Standard
Azure Container App-Umgebungen sollten keinen uneingeschränkten NSG-Zugriff haben	`microsoft.app/containerapps`	Bewährte Methoden für die Grundlagen von Azure
In verwalteten Azure Container App-Umgebungen sollten öffentliche IP-Adressen nicht aktiviert sein	`microsoft.app/managedenvironments`	Bewährte Methoden für die Grundlagen von Azure
Azure-Rollenzuweisungen sollten im Abonnementbereich keinen umfassenden Administratorzugriff gewähren	`microsoft.authorization/roleassignments`	Bewährte Methoden für die Grundlagen von Azure
Azure-Rollenzuweisungen sollten die Rolle „Benutzerzugriffsadministrator“ nicht gewähren	`microsoft.authorization/roleassignments`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Benutzerdefinierte Azure-Rollendefinitionen sollten keine Administratorberechtigungen mit Platzhaltern haben	`microsoft.authorization/roledefinitions`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Richtlinienzuweisungen für Microsoft Cloud Security Benchmark sollte der Erzwingungsmodus aktiviert sein	`microsoft.authorization/policyassignments`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Kubernetes Service (AKS) -Cluster sollten keine öffentlich zugänglichen API-Server ohne IP-Einschränkungen haben	`microsoft.containerservice/managedclusters`	Bewährte Methoden für die Grundlagen von Azure
Azure Kubernetes Service (AKS) -Cluster sollten Kubernetes-Geheimnisse im Ruhezustand verschlüsseln	`microsoft.containerservice/managedclusters`	Bewährte Methoden für die Grundlagen von Azure
Azure Kubernetes Service (AKS) -Cluster sollten eine unterstützte Kubernetes-Version ausführen	`microsoft.containerservice/managedclusters`	Bewährte Methoden für die Grundlagen von Azure

Titel des Steuerelements	Ressourcentyp	Standard
Für Azure Cosmos DB-Konten sollte die kontinuierliche Sicherung aktiviert sein	`microsoft.documentdb/databaseaccounts`	Bewährte Methoden für die Grundlagen von Azure
Bei flexiblen Azure Database for MySQL-Servern sollte der öffentliche Netzwerkzugriff deaktiviert sein	`microsoft.dbformysql/flexibleservers`	Bewährte Methoden für die Grundlagen von Azure
Azure Databricks-Arbeitsbereiche sollten in einem vom Kunden verwalteten virtuellen Netzwerk bereitgestellt werden	`microsoft.databricks/workspaces`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Databricks-Arbeitsbereiche sollte die Diagnoseprotokollzustellung konfiguriert sein	`microsoft.databricks/workspaces`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Databricks-Workspaces sollten vom Kunden verwaltete Schlüssel für die verwaltete Festplattenverschlüsselung verwenden	`microsoft.databricks/workspaces`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Microsoft Entra ID-Autorisierungsrichtlinien sollten Standardbenutzern verbieten, Anwendungen zu registrieren	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Entra ID sollten die Sicherheitsstandards aktiviert sein	`microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Microsoft Entra-Mandanten sollten über eine Richtlinie für bedingten Zugriff verfügen, die den Zugriff von unzulässigen geografischen Standorten aus blockiert	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Microsoft Entra-Mandanten sollten über eine Richtlinie für bedingten Zugriff verfügen, die den Authentifizierungsfluss für Gerätecodes blockiert	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Richtlinien für bedingten Zugriff sollten MFA für alle Benutzer vorschreiben	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Microsoft Entra-Mandanten sollten eine Multifaktorauthentifizierung für riskante Anmeldungen im Rahmen einer Richtlinie für bedingten Zugriff verlangen	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Mandanten sollten MFA über bedingten Zugriff für die Azure Service Management-API benötigen	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für mindestens eine Richtlinie mit bedingtem Zugriff sollte MFA für Microsoft Admin Portals erforderlich sein	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Autorisierungsrichtlinien von Microsoft Entra sollten Benutzer ohne Administratorrechte daran hindern, Mandanten zu erstellen	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Richtlinien für Microsoft Entra ID-Authentifizierungsmethoden sollten den Zeitraum für die erneute Bestätigung auf einen Wert ungleich Null festlegen.	`microsoft.graph/policies/authenticationmethodspolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Autorisierungsrichtlinien von Microsoft Entra sollten die Zustimmung der Benutzer für Anwendungen einschränken	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Die Azure-Autorisierungsrichtlinien sollten die Zustimmung von Benutzern auf verifizierte Herausgeber-Apps beschränken	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Autorisierungsrichtlinien von Microsoft Entra sollten den Zugriff von Gastbenutzern auf ihre eigenen Verzeichnisobjekte einschränken	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Azure-Autorisierungsrichtlinien sollten Gasteinladungen nur auf Administratorrollen beschränken	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Azure-Autorisierungsrichtlinien sollten die Erstellung von Sicherheitsgruppen auf Administratoren beschränken	`microsoft.graph/policies/authorizationpolicy`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Microsoft Entra-Mandanten sollten eine Multi-Faktor-Authentifizierung benötigen, um Geräte zu registrieren oder ihnen beizutreten	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Microsoft Entra ID-Verzeichnisrollen sollten zwischen 2 und 4 globale Administratoren haben	`microsoft.graph/directoryrole`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Die Gruppeneinstellungen von Azure Entra ID sollten die Gruppenerstellung auf Administratoren beschränken	`microsoft.graph/organization`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Abonnements sollte eine Diagnoseeinstellung für Aktivitätsprotokolle konfiguriert sein	`microsoft.insights/diagnosticsettings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für die Richtlinienzuweisung enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für das Löschen von Richtlinienzuweisungen enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für Vorgänge zum Erstellen oder Aktualisieren von Network Security Group-Vorgängen enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für das Löschen der Network Security Group enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für die Erstellung oder Aktualisierung der Sicherheitslösung enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für das Löschen der Sicherheitslösung enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für die Erstellung oder Aktualisierung von SQL Server-Firewallregeln enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für das Löschen von SQL Server-Firewallregeln enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Für Azure-Abonnements sollte eine Aktivitätsprotokollwarnung für Vorgänge zum Erstellen oder Aktualisieren einer öffentlichen IP-Adresse konfiguriert sein	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für das Löschen öffentlicher IP-Adressen enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten eine Aktivitätsprotokollwarnung für Service Health-Vorfälle enthalten	`microsoft.insights/activitylogalerts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Abonnements sollte mindestens eine Application Insights-Komponente konfiguriert sein	`microsoft.insights/components`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vaults sollte der Soft Delete- und Purge-Schutz aktiviert sein	`microsoft.keyvault/vaults`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vaults sollte die rollenbasierte Zugriffskontrolle aktiviert sein	`microsoft.keyvault/vaults`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure Key Vaults sollte der öffentliche Netzwerkzugriff deaktiviert sein, wenn private Endpunkte verwendet werden	`microsoft.keyvault/vaults`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Key Vaults sollten private Endpunkte verwenden	`microsoft.keyvault/vaults`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vaults sollte der Löschschutz aktiviert sein	`microsoft.keyvault/vaults`	Bewährte Methoden für die Grundlagen von Azure

Titel des Steuerelements	Ressourcentyp	Standard
Azure Key Vaults sollte den Netzwerkzugriff einschränken	`microsoft.keyvault/vaults`	Bewährte Methoden für die Grundlagen von Azure
Für Azure Key Vaults sollte die Protokollierung aktiviert sein AuditEvent	`microsoft.keyvault/vaults`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vault-Schlüssel in RBAC-Tresoren sollte ein Ablaufdatum festgelegt werden	`microsoft.keyvault/vaults/keys`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vault-Schlüssel in Tresoren ohne RBAC sollte ein Ablaufdatum festgelegt werden	`microsoft.keyvault/vaults/keys`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vault-Geheimnisse in RBAC-enabled Tresoren sollte ein Ablaufdatum festgelegt werden	`microsoft.keyvault/vaults/secrets`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vault-Geheimnisse in Tresoren ohne RBAC sollte ein Ablaufdatum festgelegt werden	`microsoft.keyvault/vaults/secrets`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Key Vault-Schlüssel sollte die automatische Rotation aktiviert sein	`microsoft.keyvault/vaults/keys`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Netzwerksicherheitsgruppen sollten den eingehenden RDP-Zugriff aus dem Internet einschränken	`microsoft.network/networksecuritygroups`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Netzwerksicherheitsgruppen sollten den eingehenden UDP-Zugriff aus dem Internet einschränken	`microsoft.network/networksecuritygroups`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Azure-Netzwerksicherheitsgruppen sollten den eingehenden HTTP-Zugriff aus dem Internet einschränken	`microsoft.network/networksecuritygroups`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Application Gateway-Subnetze sollten keinen uneingeschränkten NSG-Zugriff haben	`microsoft.network/networksecuritygroups`	Bewährte Methoden für die Grundlagen von Azure
Für Azure-Netzwerksicherheitsgruppen sollte eine explizite „Alles verweigern“ -Regel gelten	`microsoft.network/networksecuritygroups`	Bewährte Methoden für die Grundlagen von Azure
Azure-Netzwerksicherheitsgruppen sollten keinen uneingeschränkten eingehenden Zugriff auf eingeschränkte Ports zulassen	`microsoft.network/networksecuritygroups`	Bewährte Methoden für die Grundlagen von Azure
In den Azure Network Watcher-Flussprotokollen sollte die Protokollierung virtueller Netzwerkflüsse aktiviert sein, wobei die Datenverkehrsanalysen an Log Analytics gesendet werden	`microsoft.network/networkwatchers/flowlogs`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Netzwerksicherheitsgruppen sollten den SSH-Zugriff aus dem Internet einschränken	`microsoft.network/networksecuritygroups`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Abonnements sollten mindestens einen Azure Bastion-Host haben	`microsoft.network/bastionhosts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender für Server aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Auf Maschinen sollte eine funktionsfähige Lösung zur Schwachstellenbeurteilung in Microsoft Defender for Cloud implement iert sein	`microsoft.security/assessments`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte die Endpoint Protection-Integration mit Microsoft Defender for Cloud aktiviert sein	`microsoft.security/settings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte das agentenlose Scannen für Computer in Microsoft Defender for Servers aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte die Überwachung der Dateiintegrität in Defender for Servers aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Für das Azure-Abonnement sollte Microsoft Defender for Containers aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte Microsoft Defender for Storage aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte Microsoft Defender für App Service aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen
Bei Azure-Abonnements sollte Microsoft Defender für Azure Cosmos DB aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen

Titel des Steuerelements	Ressourcentyp	Standard
Bei Azure-Abonnements sollte Microsoft Defender für relationale Open-Source-Datenbanken aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender für Azure SQL-Datenbanken aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender für SQL Servers auf Computern aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender for Key Vault aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender für Resource Manager aktiviert sein	`microsoft.security/pricings`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei virtuellen Maschinen sollten Systemupdatebewertungen von Microsoft Defender for Cloud als fehlerfrei gemeldet werden	`microsoft.security/assessments`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Sicherheitskontakte von Microsoft Defender for Cloud sollten die Rolle „Besitzer“ über Warnmeldungen informieren	`microsoft.security/securitycontacts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Sicherheitskontakte in Microsoft Defender for Cloud sollte eine zusätzliche E-Mail-Adresse konfiguriert sein	`microsoft.security/securitycontacts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Für Azure-Sicherheitskontakte sollten E-Mail-Benachrichtigungen mit einem ausreichend umfassenden Mindestschweregrad aktiviert sein	`microsoft.security/securitycontacts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Sicherheitskontakte sollten E-Mail-Benachrichtigungen über den Angriffspfad aktiviert und eine Risikostufe konfiguriert sein	`microsoft.security/securitycontacts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure-Abonnements sollte Microsoft Defender für IoT aktiviert sein	`microsoft.security/iotsecuritysolutions`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Auf Azure SQL-Servern sollte der öffentliche Netzwerkzugriff deaktiviert sein	`microsoft.sql/servers`	Bewährte Methoden für die Grundlagen von Azure
Für SQL-Server sollte ein Azure Active Directory-Administrator konfiguriert sein	`microsoft.sql/servers`	Bewährte Methoden für die Grundlagen von Azure
Für Azure SQL-Datenbanken sollte die georedundante Sicherung aktiviert sein	`microsoft.sql/servers/databases`	Bewährte Methoden für die Grundlagen von Azure
Azure SQL-Server sollten keine standardmäßigen Administratorkonto namen verwenden	`microsoft.sql/servers`	Bewährte Methoden für die Grundlagen von Azure
Für verwaltete Azure SQL-Instanzen sollte das automatische Upgrade der Nebenversion aktiviert sein	`microsoft.sql/managedinstances`	Bewährte Methoden für die Grundlagen von Azure

Titel des Steuerelements	Ressourcentyp	Standard
Azure-Speicherkonten sollten vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei den Dateidiensten für Azure Storage-Konten sollte Soft Delete für Dateifreigaben aktiviert sein	`microsoft.storage/storageaccounts/fileservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Dateifreigaben von Azure Storage-Konten sollten SMB-Protokollversionen auf SMB 3.1.1 beschränken	`microsoft.storage/storageaccounts/fileservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten einen sicheren SMB-Kanalverschlüsselungsalgorithmus für Dateifreigaben verwenden	`microsoft.storage/storageaccounts/fileservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Storage-Konten sollte eine Erinnerung an die Schlüsselrotation konfiguriert sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Storage-Konten sollte der gemeinsame Schlüsselzugriff deaktiviert sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten private Endpunkte für den Zugriff verwenden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure Storage-Konten sollte der öffentliche Netzwerkzugriff deaktiviert sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure-Storage-Konten sollte der standardmäßige Netzwerkzugriff auf Verweigern eingestellt sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Speicherkonten sollten standardmäßig die Microsoft Entra-Autorisierung im Azure-Portal verwenden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten eine sichere Übertragung erfordern	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten es vertrauenswürdigen Azure-Diensten ermöglichen, Netzwerkregeln zu umgehen	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten mit der erforderlichen TLS-Mindestversion konfiguriert werden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei Azure Storage-Konten sollte die mandantenübergreifende Replikation deaktiviert sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für Azure Storage-Konten sollte der anonyme Blob-Zugriff deaktiviert sein	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Storage-Konten sollten das permanente Löschen von Blobs einschränken	`microsoft.storage/storageaccounts/blobservices`	Bewährte Methoden für die Grundlagen von Azure
Azure-Speicherkonten, die Aktivität sprotokolle enthalten, sollten mit einem vom Kunden verwalteten Schlüssel verschlüsselt werden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen

Titel des Steuerelements	Ressourcentyp	Standard
Bei den Blob-Diensten für Azure-Speicherkonten sollte Blob Soft Delete aktiviert sein	`microsoft.storage/storageaccounts/blobservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Für die Blob-Dienste für Azure-Speicherkonten sollte die Versionsverwaltung aktiviert sein	`microsoft.storage/storageaccounts/blobservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Bei den Blob-Diensten für Azure-Speicherkonten sollten Blob und Container Soft Delete aktiviert sein	`microsoft.storage/storageaccounts/blobservices`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Auf Azure-Speicherkonten sollte eine Azure Resource Manager-Löschsperre angewendet werden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Storage-Konten sollten über eine ReadOnly Resource Manager-Sperre verfügen	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure-Storage-Konten sollten georedundanten Speicher verwenden	`microsoft.storage/storageaccounts`	CIS Benchmark v4.0 für Microsoft Azure-Stiftungen
Azure Function-Apps sollten den administrativen Zugriff einschränken	`microsoft.web/sites/config`	Bewährte Methoden für die Grundlagen von Azure
Azure Functions sollte keinen anonymen HTTP-Triggeraufruf zulassen	`microsoft.web/sites/functions`	Bewährte Methoden für die Grundlagen von Azure
Azure App Service-Web-Apps und Funktions-Apps sollten keine nicht unterstützten Laufzeitversionen verwenden	`microsoft.web/sites`	Bewährte Methoden für die Grundlagen von Azure

Titel des Steuerelements	Ressourcentyp	Standard
Azure Function-Apps mit Premium- oder Dedicated-Plänen sollten in ein virtuelles Netzwerk integriert werden	`microsoft.web/sites`	Bewährte Methoden für die Grundlagen von Azure
Für Azure App Service-Web-Apps sollten HTTP-Protokolle in den Diagnosee instellungen aktiviert sein	`microsoft.web/sites`	CIS Benchmark v4.0 für Microsoft Azure-Sti ftungen

Löschen eines Microsoft Azure-Connectors in Security Hub CSPM

Nachdem Sie einen Microsoft Azure-Connector in AWS Security Hub CSPM erstellt haben, können Sie ihn jederzeit löschen. Wenn Sie einen Connector löschen, beendet Security Hub CSPM die Durchführung von Statusverwaltungsprüfungen und die Überwachung von Sicherheitslücken für Ihre Azure-Umgebung. Security Hub CSPM generiert auch keine neuen Erkenntnisse mehr über Ihre Umgebung. Ihre vorhandenen Ergebnisse werden 90 Tage lang aufbewahrt. Das Ressourceninventar bleibt unverändert, wie es war, als der Connector gelöscht wurde, und wird nach 90 Tagen entfernt.

Beachten Sie beim Löschen eines Connectors Folgendes:

- Security Hub CSPM löscht die Azure-Anwendungsregistrierung und die Event Hub-Infrastruktur in Ihrer Azure-Umgebung nicht. Sie müssen diese manuell direkt in Microsoft Azure löschen. Wie das geht, erfahren Sie in der Microsoft Azure-Dokumentation unter Eine Anwendung entfernen.
- Wenn es sich bei dem Connector um einen vom Kunden verwalteten Connector handelt und es auch einen dienstbezogenen Connector gibt, wirkt sich das Löschen des kundenverwalteten Connectors nicht auf den dienstbezogenen Connector aus. Security Hub CSPM erhält weiterhin Erkenntnisse zur Statusverwaltung über den serviceverknüpften Connector.
- Bestehende Ergebnisse werden innerhalb von 3—5 Tagen in einen archivierten Zustand überführt und nach Ablauf der 90-tägigen Aufbewahrungsfrist gelöscht.

Um einen Azure-Connector zu löschen

1. Öffnen Sie die Security Hub CSPM-Konsole.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie Ihren Connector aus.

4. Wählen Sie Löschen aus.
5. Bestätigen Sie, dass Sie den Connector löschen möchten, wenn Sie dazu aufgefordert werden.

Nach dem Löschen können Sie optional die Azure-Ressourcen bereinigen, die während der Installation erstellt wurden:

- Löschen Sie die App-Registrierung in Microsoft Entra ID.
- Löschen Sie den Event Hub-Namespace und die Ressourcengruppe.
- Entfernen Sie die Diagnoseeinstellungen, die Aktivitätsprotokolle und Entra ID-Prüfprotokolle exportieren.

Ergebnisse in Security Hub CSPM erstellen und aktualisieren

In AWS Security Hub CSPM ist ein Befund eine beobachtbare Aufzeichnung einer Sicherheitsüberprüfung oder einer sicherheitsrelevanten Entdeckung. Ein Befund kann aus einer der folgenden Quellen stammen:

- Eine Sicherheitsüberprüfung für ein Steuerelement in Security Hub CSPM.
- Eine Integration mit einem anderen. AWS-Service
- Eine Integration mit einem Drittanbieterprodukt.
- Eine benutzerdefinierte Integration.

Security Hub CSPM normalisiert Ergebnisse aus allen Quellen in eine Standardsyntax und ein Standardformat, das als AWS Security Finding Format (ASFF) bezeichnet wird. Ausführliche Informationen zu diesem Format, einschließlich Beschreibungen der einzelnen ASFF-Felder, finden Sie unter. AWS Format für Sicherheitssuche (ASFF) Wenn Sie die regionsübergreifende Aggregation aktivieren, aggregiert Security Hub CSPM auch automatisch neue und aktualisierte Ergebnisse aus allen verknüpften Regionen in eine von Ihnen angegebene Aggregationsregion. Weitere Informationen finden Sie unter Grundlegendes zur regionsübergreifenden Aggregation in Security Hub CSPM.

Nachdem ein Ergebnis erstellt wurde, kann es wie folgt aktualisiert werden:

- Ein Findungsanbieter kann den BatchImportFindingsBetrieb der Security Hub CSPM-API verwenden, um allgemeine Informationen über das Ergebnis zu aktualisieren. Ergebnisanbieter können nur Ergebnisse aktualisieren, die sie erstellt haben.

- Ein Kunde kann die Security Hub CSPM-Konsole oder den BatchUpdateFindingsBetrieb der Security Hub CSPM-API verwenden, um den Status der Untersuchung des Ergebnisses zu aktualisieren. Der `BatchUpdateFindings` Vorgang kann auch von einem SIEM-, Ticketing-, Incident Management-, SOAR- oder anderen Tools im Namen eines Kunden genutzt werden.

Security Hub CSPM löscht automatisch Ergebnisse, die in letzter Zeit nicht aktualisiert wurden, um das Auffinden zu reduzieren und die Nachverfolgung und Analyse einzelner Ergebnisse zu optimieren. Der Zeitpunkt, zu dem Security Hub CSPM dies tut, hängt davon ab, ob ein Ergebnis aktiv oder archiviert ist:

- Ein aktives Ergebnis ist ein Befund, dessen Datensatzstatus (`RecordState`) ist. `ACTIVE` Security Hub CSPM speichert aktive Ergebnisse 90 Tage lang. Wenn ein aktives Ergebnis 90 Tage lang nicht aktualisiert wurde, läuft es ab und Security Hub CSPM löscht es dauerhaft.
- Ein archiviertes Ergebnis ist ein Befund mit dem Datensatzstatus ()`RecordState`. `ARCHIVED` Security Hub CSPM speichert archivierte Ergebnisse 30 Tage lang. Wenn ein archiviertes Ergebnis 30 Tage lang nicht aktualisiert wurde, läuft es ab und Security Hub CSPM löscht es dauerhaft.

Bei Kontrollergebnissen, d. h. Ergebnissen, die Security Hub CSPM aus Sicherheitsprüfungen für Kontrollen generiert, bestimmt Security Hub CSPM anhand des Werts für das `UpdatedAt` Feld des Ergebnisses, ob ein Ergebnis abgelaufen ist. Wenn dieser Wert für einen aktiven Befund mehr als 90 Tage zurückliegt, löscht Security Hub CSPM den Befund dauerhaft. Wenn dieser Wert für einen archivierten Befund vor mehr als 30 Tagen lag, löscht Security Hub CSPM den Befund dauerhaft.

Für alle anderen Arten von Ergebnissen bestimmt Security Hub CSPM anhand der Werte für die `UpdatedAt` Felder `ProcessedAt` und des Ergebnisses, ob ein Ergebnis abgelaufen ist. Security Hub CSPM vergleicht die Werte für diese Felder und ermittelt, welcher aktueller ist. Wenn der neuere Wert für ein aktives Ergebnis mehr als 90 Tage zurückliegt, löscht Security Hub CSPM das Ergebnis dauerhaft. Wenn der neuere Wert für ein archiviertes Ergebnis mehr als 30 Tage zurückliegt, löscht Security Hub CSPM das Ergebnis dauerhaft. Die Suche nach Anbietern kann den Wert für das `UpdatedAt` Feld eines oder mehrerer Ergebnisse mithilfe der BatchImportFindingsSecurity Hub CSPM-API ändern.

Für eine längerfristige Aufbewahrung von Ergebnissen können Sie Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter Verwendung EventBridge für automatische Reaktionen und Problembehebungen.

Themen

- BatchImportFindings um Anbieter zu finden
- BatchUpdateFindings für Kunden
- Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM
- Ergebnisse im Security Hub CSPM filtern
- Gruppierung der Ergebnisse in Security Hub CSPM
- Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen
- Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden
- AWS Format für Sicherheitssuche (ASFF)

BatchImportFindings um Anbieter zu finden

Finding Provider können den BatchImportFindingsVorgang nutzen, um neue Erkenntnisse in AWS Security Hub CSPM zu erstellen. Sie können diesen Vorgang auch verwenden, um die von ihnen erstellten Ergebnisse zu aktualisieren. Die Suche nach Anbietern kann keine Ergebnisse aktualisieren, die sie nicht selbst erstellt haben.

Kunden, SIEMs, Ticketing, SOAR und andere Arten von Tools müssen den BatchUpdateFindingsVorgang nutzen, um Aktualisierungen im Zusammenhang mit ihrer Untersuchung der Ergebnisse aus der Suche nach Anbietern vorzunehmen. Weitere Informationen finden Sie unter the section called “BatchUpdateFindings für Kunden”.

Wenn Security Hub CSPM eine `BatchImportFindings` Anfrage zur Erstellung oder Aktualisierung eines Ergebnisses erhält, generiert es automatisch ein Security Hub Findings - ImportedEreignis in Amazon. EventBridge Sie können bei diesem Ereignis automatisierte Maßnahmen ergreifen. Weitere Informationen finden Sie unter the section called “Automatisierte Reaktion und Problembehebung”.

Voraussetzungen für die Verwendung von **`BatchImportFindings`**

`BatchImportFindings`muss von einer der folgenden Personen aufgerufen werden:

- Das Konto, das mit den Ergebnissen verknüpft ist. Die Kennung des verknüpften Kontos muss mit dem Wert des `AwsAccountId` Attributs für den Befund übereinstimmen.
- Ein Konto, das als offizielle Security Hub CSPM-Partnerintegration zugelassen ist.

Security Hub CSPM kann nur die Suche nach Updates für Konten akzeptieren, für die Security Hub CSPM aktiviert ist. Der Ergebnisanbieter muss ebenfalls aktiviert sein. Wenn Security Hub CSPM deaktiviert oder die Finding Provider-Integration nicht aktiviert ist, werden die Ergebnisse in der `FailedFindings` Liste mit einem `InvalidAccess` Fehler zurückgegeben.

Festlegen, ob ein Ergebnis erstellt oder aktualisiert werden soll

Um festzustellen, ob ein Ergebnis erstellt oder aktualisiert werden soll, überprüft Security Hub CSPM das `ID` Feld. Wenn der Wert von `ID` nicht mit einem vorhandenen Ergebnis übereinstimmt, erstellt Security Hub CSPM ein neues Ergebnis.

Wenn es `ID` mit einem vorhandenen Ergebnis übereinstimmt, überprüft Security Hub CSPM das `UpdatedAt` Feld auf das Update und geht wie folgt vor:

- Wenn das Update mit `UpdatedAt` dem vorhandenen Ergebnis übereinstimmt oder davor `UpdatedAt` auftritt, ignoriert Security Hub CSPM die Aktualisierungsanfrage.
- Wenn `UpdatedAt` das Update nach `UpdatedAt` dem vorhandenen Befund erfolgt, aktualisiert Security Hub CSPM den vorhandenen Befund.

Einschränkungen beim Auffinden von Updates mit **`BatchImportFindings`**

Die Suche nach Anbietern kann nicht verwendet `BatchImportFindings` werden, um die folgenden Attribute eines vorhandenen Ergebnisses zu aktualisieren:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM ignoriert alle Inhalte, die in einer `BatchImportFindings` Anfrage für diese Attribute bereitgestellt werden. Kunden oder in ihrem Namen handelnde Unternehmen (z. B. Ticketing-Tools) können diese Attribute verwenden, `BatchUpdateFindings` um sie zu aktualisieren.

Aktualisierung der Ergebnisse mit FindingProviderFields

Finding Providers sollte außerdem nicht verwendet werden`BatchImportFindings`, um die folgenden Top-Level-Attribute im AWS Security Finding Format (ASFF) zu aktualisieren:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Stattdessen sollte die Suche nach Anbietern das `FindingProviderFields`Objekt verwenden, um Werte für diese Attribute bereitzustellen.

Beispiel

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Bei `BatchImportFindings` Anfragen verarbeitet Security Hub CSPM Werte in den Attributen der obersten Ebene und wie folgt. `FindingProviderFields`

(Preferred) **`BatchImportFindings`** liefert einen Wert für ein Attribut in **`FindingProviderFields`**, aber keinen Wert für das entsprechende Attribut der obersten Ebene.

Zum Beispiel `BatchImportFindings` liefert`FindingProviderFields.Confidence`, aber nicht. `Confidence` Dies ist die bevorzugte Option für `BatchImportFindings` Anfragen.

Security Hub CSPM aktualisiert den Wert des Attributs in. `FindingProviderFields`

Es repliziert den Wert nur dann in das Attribut der obersten Ebene, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

`BatchImportFindings`liefert einen Wert für ein Attribut der obersten Ebene, aber keinen Wert für das entsprechende Attribut in. **`FindingProviderFields`**

Stellt beispielsweise `BatchImportFindings` bereit`Confidence`, liefert aber nicht. `FindingProviderFields.Confidence`

Security Hub CSPM verwendet den Wert, um das Attribut in zu aktualisieren. `FindingProviderFields` Es überschreibt jeden vorhandenen Wert.

Security Hub CSPM aktualisiert das Attribut der obersten Ebene nur, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

`BatchImportFindings`stellt einen Wert sowohl für ein Attribut der obersten Ebene als auch für das entsprechende Attribut in bereit. **`FindingProviderFields`**

`BatchImportFindings`Stellt beispielsweise sowohl als auch `Confidence` bereit. `FindingProviderFields.Confidence`

Für ein neues Ergebnis verwendet Security Hub CSPM den Wert in, `FindingProviderFields` um sowohl das oberste Ebenenattribut als auch das entsprechende Attribut in aufzufüllen. `FindingProviderFields` Der angegebene Attributwert der obersten Ebene wird nicht verwendet.

Für ein vorhandenes Ergebnis verwendet Security Hub CSPM beide Werte. Der Attributwert der obersten Ebene wird jedoch nur aktualisiert, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

BatchUpdateFindings für Kunden

AWS Security Hub CSPM-Kunden und in ihrem Namen handelnde Unternehmen können den BatchUpdateFindingsVorgang nutzen, um Informationen im Zusammenhang mit der Verarbeitung von Security Hub CSPM-Ergebnissen von suchenden Anbietern zu aktualisieren. Als Kunde können Sie diesen Vorgang direkt nutzen. SIEM-, Ticketing-, Incident Management- und SOAR-Tools können diesen Vorgang auch im Auftrag eines Kunden nutzen.

Sie können den `BatchUpdateFindings` Vorgang nicht verwenden, um neue Erkenntnisse zu gewinnen. Sie können damit jedoch bis zu 100 vorhandene Ergebnisse gleichzeitig aktualisieren. In einer `BatchUpdateFindings` Anfrage geben Sie an, welche Ergebnisse aktualisiert werden sollen, welche ASFF-Felder (AWS Security Finding Format) für die Ergebnisse aktualisiert werden sollen,

und die neuen Werte für die Felder. Security Hub CSPM aktualisiert dann die Ergebnisse wie in Ihrer Anfrage angegeben. Dieser Vorgang kann einige Minuten dauern. Wenn Sie die Ergebnisse mithilfe des `BatchUpdateFindings` Vorgangs aktualisieren, wirken sich Ihre Aktualisierungen nicht auf die vorhandenen Werte für das `UpdatedAt` Ergebnisfeld aus.

Wenn Security Hub CSPM eine `BatchUpdateFindings` Anfrage zur Aktualisierung eines Ergebnisses erhält, generiert es automatisch ein Security Hub Findings – ImportedEreignis in Amazon. EventBridge Sie können dieses Ereignis optional verwenden, um automatisierte Maßnahmen in Bezug auf das angegebene Ergebnis zu ergreifen. Weitere Informationen finden Sie unter the section called “Automatisierte Reaktion und Problembehebung”.

Verfügbare Felder für BatchUpdateFindings

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, können Sie `BatchUpdateFindings` damit Ergebnisse aktualisieren, die vom Administratorkonto oder den Mitgliedskonten generiert wurden. Mitgliedskonten können nur `BatchUpdateFindings` zur Aktualisierung der Ergebnisse für ihr Konto verwendet werden.

Kunden können `BatchUpdateFindings` damit die folgenden Felder und Objekte aktualisieren:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Konfiguration des Zugriffs auf BatchUpdateFindings

Sie können AWS Identity and Access Management (IAM-) Richtlinien konfigurieren, um den Zugriff auf die Verwendung `BatchUpdateFindings` zur Aktualisierung von Suchfeldern und Feldwerten einzuschränken.

Verwenden Sie in einer Anweisung, auf die der Zugriff beschränkt werden sollBatchUpdateFindings, die folgenden Werte:

- Action ist securityhub:BatchUpdateFindings
- Effect ist Deny
- Denn Condition Sie können eine BatchUpdateFindings Anfrage auf folgender Grundlage ablehnen:
  - Das Ergebnis umfasst ein bestimmtes Feld.
  - Das Ergebnis beinhaltet einen bestimmten Feldwert.

Bedingungsschlüssel

Dies sind die Bedingungsschlüssel für die Einschränkung des Zugriffs aufBatchUpdateFindings.

ASFF-Feld

Der Bedingungsschlüssel für ein ASFF-Feld lautet wie folgt:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ersetzen Sie es *<fieldName>* durch das ASFF-Feld. Fügen Sie bei der Konfiguration des Zugriffs auf BatchUpdateFindings ein oder mehrere spezifische ASFF-Felder in Ihre IAM-Richtlinie ein und nicht ein Feld auf übergeordneter Ebene. Um beispielsweise den Zugriff auf das Workflow.Status Feld einzuschränken, müssen Sie es securityhub:ASFFSyntaxPath/Workflow.Status in Ihre Richtlinie aufnehmen und nicht das Feld auf übergeordneter Ebene. Workflow

Alle Aktualisierungen eines Felds verbieten

Um zu verhindern, dass ein Benutzer ein bestimmtes Feld aktualisiert, verwenden Sie eine Bedingung wie die folgende:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Die folgende Aussage weist beispielsweise darauf hin, dass das `Workflow.Status` Ergebnisfeld nicht aktualisiert werden `BatchUpdateFindings` kann.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Bestimmte Feldwerte nicht zulassen

Um zu verhindern, dass ein Benutzer ein Feld auf einen bestimmten Wert setzt, verwenden Sie eine Bedingung wie die folgende:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass diese Einstellung nicht verwendet werden `BatchUpdateFindings` kann, um auf `Workflow.Status` zu setzen`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Sie können auch eine Liste mit Werten angeben, die nicht zulässig sind.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass dieser Wert nicht verwendet werden `BatchUpdateFindings` kann, um entweder `Workflow.Status` auf `RESOLVED` oder zu setzen`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM

In AWS Security Hub CSPM ist ein Befund eine beobachtbare Aufzeichnung einer Sicherheitsüberprüfung oder einer sicherheitsrelevanten Entdeckung. Security Hub CSPM generiert ein Ergebnis, wenn es eine Sicherheitsüberprüfung einer Kontrolle abschließt und wenn es ein Ergebnis aus einem integrierten Produkt AWS-Service oder einem Drittanbieterprodukt aufnimmt. Jedes Ergebnis enthält eine Historie der Änderungen und weitere Details, wie z. B. eine Bewertung des Schweregrads und Informationen zu den betroffenen Ressourcen.

Sie können den Verlauf und andere Details einzelner Ergebnisse auf der Security Hub CSPM-Konsole oder programmgesteuert mit der Security Hub CSPM-API oder dem überprüfen. AWS CLI

Um Ihnen bei der Optimierung Ihrer Analyse zu helfen, zeigt die Security Hub CSPM-Konsole ein Ergebnisfenster an, wenn Sie ein bestimmtes Ergebnis auswählen. Das Fenster umfasst verschiedene Menüs und Registerkarten zur Überprüfung bestimmter Details eines Ergebnisses.

Menü „Aktionen“

In diesem Menü können Sie die vollständige JSON-Datei eines Befundes überprüfen oder Notizen hinzufügen. Einem Befund kann jeweils nur eine Notiz angehängt werden. Dieses Menü bietet auch Optionen, um den Workflow-Status eines Ergebnisses festzulegen oder ein Ergebnis an eine benutzerdefinierte Aktion in Amazon zu senden EventBridge.

Menü „Untersuchen“

In diesem Menü können Sie einen Befund in Amazon Detective untersuchen. Detective extrahiert Entitäten wie IP-Adressen und AWS Benutzer aus einem Befund und visualisiert deren Aktivitäten. Sie können die Entitätsaktivität als Ausgangspunkt verwenden, um die Ursache und die Auswirkung eines Ergebnisses zu untersuchen.

Registerkarte Übersicht

Diese Registerkarte enthält eine Zusammenfassung eines Ergebnisses. Sie können beispielsweise ermitteln, wann ein Ergebnis erstellt und zuletzt aktualisiert wurde, in welchem Konto es vorhanden ist und aus welcher Quelle das Ergebnis stammt. Bei Kontrollergebnissen werden auf dieser Registerkarte auch der Name der zugehörigen AWS Config Regel und ein Link zu Anleitungen zur Problembehebung in der Security Hub CSPM-Dokumentation angezeigt.

Im Ressourcen-Snapshot auf der Registerkarte Übersicht können Sie sich einen kurzen Überblick über die Ressourcen verschaffen, die an einem Befund beteiligt waren. Bei einigen Ressourcen umfasst dies die Option „Ressource öffnen“, die direkt zu einer betroffenen Ressource auf der entsprechenden AWS-Service Konsole führt. In der Momentaufnahme des Verlaufs werden bis zu zwei Änderungen an dem Ergebnis angezeigt, die an dem letzten Tag vorgenommen wurden, für den der Verlauf nachverfolgt wird. Wenn Sie beispielsweise gestern eine Änderung und heute eine weitere vorgenommen haben, zeigt der Snapshot die Änderung von heute. Um frühere Einträge zu überprüfen, wechseln Sie zur Registerkarte Verlauf.

Die Zeile Konformität wird erweitert, um weitere Details anzuzeigen. Wenn ein Steuerelement beispielsweise Parameter enthält, können Sie die Parameterwerte überprüfen, die Security Hub CSPM derzeit bei der Durchführung von Sicherheitsprüfungen für das Steuerelement verwendet.

Registerkarte „Ressourcen“

Auf dieser Registerkarte finden Sie Einzelheiten zu den Ressourcen, die an einem Befund beteiligt waren. Wenn Sie bei dem Konto angemeldet sind, dem eine Ressource gehört, können Sie die Ressource in der entsprechenden AWS-Service Konsole überprüfen. Wenn Sie nicht der Besitzer einer Ressource sind, wird auf dieser Registerkarte die AWS-Konto ID des Besitzers angezeigt.

In der Zeile Details werden ressourcenspezifische Details zu einem Ergebnis angezeigt. Sie zeigt den ResourceDetailsAbschnitt des Ergebnisses im JSON-Format.

In der Zeile „Tags“ werden Tag-Schlüssel und -Werte angezeigt, die den Ressourcen zugewiesen sind, die an einem Befund beteiligt sind. Ressourcen, die vom GetResources Betrieb der AWS -Ressourcengruppen Tagging-API unterstützt werden, können markiert werden. Security Hub CSPM ruft diesen Vorgang mithilfe einer dienstbezogenen Rolle bei der Verarbeitung neuer oder aktualisierter Ergebnisse auf und ruft die Ressourcen-Tags ab, wenn das `Resource.Id` Feld AWS Security Finding Format (ASFF) mit dem ARN einer Ressource gefüllt ist. Security Hub CSPM ignoriert ungültige Ressourcen-IDs. Weitere Informationen zur Aufnahme von Ressourcen-Tags in die Ergebnisse finden Sie unter. Tags (Markierungen)

Registerkarte „Verlauf“

Auf dieser Registerkarte wird der Verlauf eines Befundes nachverfolgt. Die Fundhistorie ist für aktive und archivierte Ergebnisse verfügbar. Es bietet eine unveränderliche Aufzeichnung der Änderungen, die im Laufe der Zeit an einem Ergebnis vorgenommen wurden, einschließlich der Änderung, welches ASFF-Feld geändert wurde, wann die Änderung vorgenommen wurde und von welchem Benutzer. Auf jeder Seite der Registerkarte werden bis zu 20 Änderungen angezeigt. Neuere Änderungen werden zuerst angezeigt.

Bei aktiven Ergebnissen ist die Fundhistorie für bis zu 90 Tage verfügbar. Für archivierte Ergebnisse ist die Fundhistorie für bis zu 30 Tage verfügbar. Der Suchverlauf umfasst Änderungen, die manuell oder automatisch durch die CSPM-Automatisierungsregeln von Security Hub vorgenommen wurden. Änderungen an Zeitstempelfeldern der obersten Ebene, wie z. B. den Feldern und, sind nicht enthalten. `CreatedAt` `UpdatedAt`

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, bezieht sich der Suchverlauf auf das Administratorkonto und alle Mitgliedskonten.

Registerkarte „Bedrohung“

Diese Registerkarte enthält Daten von ActionMalware, und ProcessDetailsObjekten der ASFF, einschließlich der Art der Bedrohung und ob es sich bei einer Ressource um das Ziel oder den Akteur handelt. Diese Angaben gelten in der Regel für Ergebnisse, die ihren Ursprung in Amazon haben GuardDuty.

Registerkarte Sicherheitslücken

Auf dieser Registerkarte werden Daten aus dem VulnerabilityObjekt des ASFF angezeigt, einschließlich Informationen darüber, ob es im Zusammenhang mit einem Befund Exploits oder

verfügbare Fixes gibt. Diese Angaben gelten in der Regel für Ergebnisse, die ihren Ursprung in Amazon Inspector haben.

Die Zeilen auf jeder Registerkarte enthalten eine Kopier- oder Filteroption. Wenn Sie beispielsweise den Bereich für ein Ergebnis öffnen, das den Workflow-Status Benachrichtigt hat, können Sie die Filteroption neben der Zeile Workflow-Status auswählen. Wenn Sie Alle Ergebnisse mit diesem Wert anzeigen wählen, filtert Security Hub CSPM die Ergebnistabelle und zeigt nur Ergebnisse mit demselben Workflow-Status an.

Details und Verlauf der Ergebnisse überprüfen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Suchdetails in Security Hub CSPM zu überprüfen.

Wenn Sie die regionsübergreifende Aggregation aktivieren und sich bei der Aggregationsregion anmelden, umfasst die Suche nach Daten auch Daten aus der Aggregationsregion und verknüpften Regionen. In anderen Regionen ist das Suchen von Daten nur für diese Region spezifisch. Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter. the section called “Aggregation von Daten über Regionen hinweg”

Security Hub CSPM console

Einzelheiten und Verlauf der Ergebnisse überprüfen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
   - Wählen Sie im Navigationsbereich Findings aus. Fügen Sie nach Bedarf Suchfilter hinzu, um die Ergebnisliste einzugrenzen.
   - Wählen Sie im Navigationsbereich Insights aus. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wählen Sie im Navigationsbereich Integrationen aus. Wählen Sie für eine Integration die Option Ergebnisse anzeigen aus.
   - Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie ein Ergebnis aus. Im Ergebnisfenster werden die Details des Ergebnisses angezeigt.
4. Führen Sie im Ergebnisfenster einen der folgenden Schritte aus:

- Wählen Sie eine Registerkarte, um spezifische Details zum Ergebnis zu überprüfen.
- Um Maßnahmen gegen das Ergebnis zu ergreifen, wählen Sie eine Option aus dem Menü „Aktionen“ aus.
- Um den Befund in Amazon Detective zu untersuchen, wählen Sie eine Option Untersuchen.

> **Note**
>
> Wenn Sie sich mit einem Mitgliedskonto integrieren AWS Organizations und dort angemeldet sind, enthält das Ergebnisfenster den Kontonamen. Für Mitgliedskonten, die manuell statt über Organizations eingeladen werden, enthält das Suchfeld nur die Konto-ID.

Security Hub CSPM API

Verwenden Sie den GetFindingsBetrieb der Security Hub CSPM-API, oder wenn Sie die verwenden AWS CLI, führen Sie den Befehl aus. get-findings Sie können einen oder mehrere Werte für den `Filters` Parameter angeben, um die abzurufenden Ergebnisse einzugrenzen.

Wenn das Volumen der Ergebnisse zu groß ist, können Sie den `MaxResults` Parameter verwenden, um die Ergebnisse auf eine bestimmte Anzahl zu beschränken, und den `NextToken` Parameter verwenden, um die Ergebnisse zu paginieren. Verwenden Sie den `SortCriteria` Parameter, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

Mit dem folgenden AWS CLI Befehl werden beispielsweise die Ergebnisse abgerufen, die den angegebenen Filterkriterien entsprechen, und die Ergebnisse werden in absteigender Reihenfolge nach dem `LastObservedAt` Feld sortiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Verwenden Sie den Vorgang, um den Verlauf der GetFindingHistoryErgebnisse zu überprüfen. Wenn Sie den verwenden AWS CLI, führen Sie den get-finding-historyBefehl aus. Identifizieren Sie das Ergebnis, für das Sie den Verlauf abrufen möchten, mit den `Id` Feldern `ProductArn` und. Informationen zu diesen Feldern finden Sie unter AwsSecurityFindingIdentifier. Jede Anfrage kann den Verlauf für nur einen Befund abrufen.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der Verlauf für den angegebenen Befund abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Verwenden Sie das cmdlet `Get-SHUBFinding`. Füllen Sie optional den `Filter` Parameter aus, um die abzurufenden Ergebnisse einzugrenzen.

Das folgende Cmdlet ruft beispielsweise die Ergebnisse ab, die den angegebenen Filtern entsprechen.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Wenn Sie Ergebnisse nach `CompanyName` oder filtern`ProductName`, verwendet Security Hub CSPM die Werte, die Teil des `ProductFields` ASFF-Objekts sind. Security Hub CSPM verwendet nicht die Felder der obersten Ebene `CompanyName` und. `ProductName`

Ergebnisse im Security Hub CSPM filtern

AWS Security Hub CSPM generiert seine eigenen Ergebnisse aus Sicherheitsprüfungen und erhält Ergebnisse aus integrierten Produkten. Sie können eine Liste der Ergebnisse auf den Seiten Findings, Integrations und Insights der Security Hub CSPM-Konsole anzeigen. Sie können Filter hinzufügen, um eine Ergebnisliste einzugrenzen, sodass die Liste für Ihre Organisation oder Ihren Anwendungsfall relevant ist.

Informationen zum Filtern von Ergebnissen für eine bestimmte Sicherheitskontrolle finden Sie unterthe section called “Filterung und Sortierung der Kontrollergebnisse”. Die Informationen auf dieser Seite gelten für die Seiten Ergebnisse, Einblicke und Integrationen.

Standardfilter für Suchlisten

Standardmäßig werden Suchlisten auf der Security Hub CSPM-Konsole anhand der `Workflow.Status` Felder `RecordState` und des AWS Security Finding Formats (ASFF) gefiltert. Dies gilt zusätzlich zu den Filtern für einen bestimmten Einblick oder eine bestimmte Integration.

Der Datensatzstatus gibt an, ob ein Ergebnis aktiv oder archiviert ist. Standardmäßig werden in einer Ergebnisliste nur aktive Ergebnisse angezeigt. Ein Anbieter von Ergebnissen kann ein Ergebnis archivieren, wenn es nicht mehr aktiv oder wichtig ist. Security Hub CSPM archiviert Kontrollergebnisse auch automatisch, wenn die zugehörige Ressource gelöscht wird.

Der Workflow-Status gibt den Status einer Untersuchung eines Ergebnisses an. Standardmäßig werden in einer Ergebnisliste nur Ergebnisse mit dem Workflow-Status `NEW` oder `NOTIFIED` angezeigt. Sie können den Workflow-Status eines Ergebnisses aktualisieren.

Anweisungen zum Hinzufügen von Filtern

Sie können eine Ergebnisliste nach bis zu zehn Attributen filtern. Für jedes Attribut können Sie bis zu 20 Filterwerte angeben.

Beim Filtern der Ergebnisliste wendet Security Hub CSPM `AND` Logik auf den Filtersatz an. Ein Ergebnis stimmt nur dann überein, wenn es allen bereitgestellten Filtern entspricht. Wenn Sie beispielsweise GuardDuty als Filter für den Produktnamen und `AwsS3Bucket` als Filter für den Ressourcentyp hinzufügen, zeigt Security Hub CSPM Ergebnisse an, die diesen beiden Kriterien entsprechen.

Security Hub CSPM wendet `OR` Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Wenn Sie beispielsweise GuardDuty sowohl als auch Amazon Inspector als Filterwerte

für den Produktnamen hinzufügen, zeigt Security Hub CSPM Ergebnisse an, die entweder von Amazon Inspector GuardDuty oder Amazon Inspector generiert wurden.

Um Filter zu einer Ergebnisliste hinzuzufügen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Um eine Ergebnisliste anzuzeigen, führen Sie im Navigationsbereich eine der folgenden Aktionen aus:
   - Wählen Sie Ergebnisse aus.
   - Wählen Sie Insights aus. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wähle Sie Integrations (Integrationen) aus. Wählen Sie Ergebnisse anzeigen für eine Integration aus.
3. Wählen Sie im Feld Filter hinzufügen ein oder mehrere Felder aus, nach denen gefiltert werden soll.

   Wenn Sie nach Firmenname oder Produktname filtern, verwendet die Konsole die `ProductName` Felder der obersten Ebene `CompanyName` und das AWS Security Finding Format (ASFF). Die API verwendet die Werte, die unter verschachtelt sind. `ProductFields`
4. Wählen Sie den Filterübereinstimmungstyp aus.

   Für einen Zeichenkettenfilter können Sie aus den folgenden Optionen wählen:

   - ist — Findet einen Wert, der genau dem Filterwert entspricht.
   - beginnt mit — Findet einen Wert, der mit dem Filterwert beginnt.
   - ist nicht — Findet einen Wert, der nicht mit dem Filterwert übereinstimmt.
   - beginnt nicht mit — Findet einen Wert, der nicht mit dem Filterwert beginnt.

   Für das Feld Ressourcen-Tags können Sie nach bestimmten Schlüsseln oder Werten filtern.

   Für einen numerischen Filter können Sie wählen, ob Sie eine einzelne Zahl (Simple) oder einen Zahlenbereich (Range) angeben möchten.

Für einen Datums- oder Uhrzeitfilter können Sie wählen, ob Sie eine Zeitspanne vom aktuellen Datum und der aktuellen Uhrzeit (Rollendes Fenster) oder einen bestimmten Datumsbereich (fester Bereich) angeben möchten.

Das Hinzufügen mehrerer Filter hat die folgenden Interaktionen:

- ist und beginnt mit Filtern werden durch OR verknüpft. Ein Wert stimmt überein, wenn er einen der Filterwerte enthält. Wenn Sie beispielsweise die Bezeichnung Schweregrad auf KRITISCH und die Bezeichnung Schweregrad auf HOCH angeben, enthalten die Ergebnisse sowohl kritische als auch Ergebnisse mit hohem Schweregrad.
- ist nicht und beginnt auch nicht mit Filtern, die durch UND verknüpft werden. Ein Wert stimmt nur überein, wenn er keinen dieser Filterwerte enthält. Wenn Sie beispielsweise angeben, dass die Bezeichnung Schweregrad nicht NIEDRIG und die Bezeichnung Schweregrad nicht MITTEL ist, enthalten die Ergebnisse keine Ergebnisse mit niedrigem oder mittlerem Schweregrad.

Wenn Sie einen Is-Filter für ein Feld verwenden, können Sie nicht den Filter Ist nicht oder A fängt nicht mit an für dasselbe Feld verwenden.

5. Geben Sie den Filterwert an. Bei Zeichenkettenfiltern unterscheidet der Filterwert zwischen Groß- und Kleinschreibung.
6. Wählen Sie Anwenden aus.

Für einen vorhandenen Filter können Sie den Übereinstimmungstyp oder den Wert des Filters ändern. Wählen Sie in einer gefilterten Ergebnisliste den Filter aus. Wählen Sie im Feld Filter bearbeiten den neuen Treffertyp oder Wert aus, und klicken Sie dann auf Anwenden.

Um einen Filter zu entfernen, wählen Sie das X-Symbol. Die Liste wird automatisch aktualisiert, um die Änderung widerzuspiegeln.

Gruppierung der Ergebnisse in Security Hub CSPM

Sie können Ergebnisse in AWS Security Hub CSPM auf der Grundlage der Werte eines ausgewählten Attributs gruppieren.

Wenn Sie die Ergebnisse gruppieren, wird die Ergebnisliste durch eine Werteliste für das ausgewählte Attribut in den entsprechenden Ergebnissen ersetzt. Für jeden Wert wird in der Liste die Anzahl der übereinstimmenden Ergebnisse angezeigt.

Wenn Sie die Ergebnisse beispielsweise nach AWS-Konto ID gruppieren, wird eine Liste von Konto-IDs mit der Anzahl der übereinstimmenden Ergebnisse für jedes Konto angezeigt.

Security Hub CSPM kann bis zu 100 Werte für ein ausgewähltes Attribut anzeigen. Wenn es mehr als 100 Werte gibt, werden nur die ersten 100 angezeigt.

Wenn Sie einen Attributwert auswählen, zeigt Security Hub CSPM die Liste der passenden Ergebnisse für diesen Wert an.

Um die Ergebnisse in einer Ergebnisliste zu gruppieren (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Um eine Ergebnisliste anzuzeigen, führen Sie im Navigationsbereich eine der folgenden Aktionen aus:
   - Wählen Sie Ergebnisse aus.
   - Wählen Sie Insights aus. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wähle Sie Integrations (Integrationen) aus. Wählen Sie Ergebnisse anzeigen für eine Integration aus.
3. Wählen Sie in der Dropdownliste Gruppieren nach das Attribut aus, das für die Gruppierung verwendet werden soll.

   Um ein Gruppierungsattribut zu entfernen, wählen Sie das X-Symbol. Wenn Sie das Gruppierungsattribut entfernen, ändert sich die Liste von der Liste der Attributwerte in eine Ergebnisliste.

Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen

Der Workflow-Status verfolgt den Fortschritt Ihrer Untersuchung zu einem Ergebnis. Der Workflow-Status ist spezifisch für ein einzelnes Ergebnis und hat keinen Einfluss auf die Generierung neuer Ergebnisse. Wenn Sie beispielsweise den Workflow-Status eines Ergebnisses auf `SUPPRESSED` oder

ändernRESOLVED, verhindert Ihre Änderung nicht, dass Security Hub CSPM ein neues Ergebnis für dasselbe Problem generiert.

Der Workflow-Status eines Befundes kann einer der folgenden Werte sein.

NEU

Der Ausgangszustand eines Ergebnisses, bevor Sie es überprüfen.

Ergebnisse, die aus integrierten Quellen aufgenommen wurden AWS-Services AWS Config, haben z. NEW B. ihren ursprünglichen Status.

Security Hub CSPM setzt in den folgenden Fällen auch den Workflow-Status von entweder NOTIFIED oder RESOLVED NEW auf zurück:

- RecordState ändert sich von ARCHIVED in ACTIVE.
- Compliance.Statusändert sich von PASSED zuFAILED, WARNING oder. NOT_AVAILABLE

Diese Änderungen bedeuten, dass zusätzliche Untersuchungen erforderlich sind.

BENACHRICHTIGT

Gibt an, dass Sie den Ressourceneigentümer über das Sicherheitsproblem informiert haben. Sie können diesen Status verwenden, wenn Sie nicht der Ressourceneigentümer sind und einen Eingriff von diesem benötigen, um ein Sicherheitsproblem zu beheben.

Wenn einer der folgenden Fälle eintritt, wird der Workflow-Status automatisch von NOTIFIED zu geändertNEW:

- RecordState ändert sich von ARCHIVED in ACTIVE.
- Compliance.Statusändert sich von PASSED zu FAILEDWARNING, oderNOT_AVAILABLE.

UNTERDRÜCKT

Zeigt an, dass Sie das Ergebnis überprüft haben und nicht der Meinung sind, dass weitere Maßnahmen erforderlich sind.

Der Workflow-Status eines SUPPRESSED Ergebnisses RecordState ändert sich nicht, wenn er von ARCHIVED zu geändert wirdACTIVE.

GELÖST

Das Ergebnis wurde überprüft und korrigiert und gilt nun als gelöst.

Der Befund bleibt bestehenRESOLVED, sofern nicht einer der folgenden Fälle eintritt:

- `RecordState` ändert sich von `ARCHIVED` in `ACTIVE`.
- `Compliance.Status`ändert sich von `PASSED` zu `FAILEDWARNING`, oder`NOT_AVAILABLE`.

In diesen Fällen wird der Workflow-Status automatisch auf zurückgesetzt`NEW`.

Falls dies der Fall `Compliance.Status` ist`PASSED`, setzt Security Hub CSPM den Workflow-Status automatisch auf. `RESOLVED`

Den Workflow-Status von Ergebnissen festlegen

Um den Workflow-Status eines oder mehrerer Ergebnisse zu ändern, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Wenn Sie den Workflow-Status eines Befundes ändern, beachten Sie, dass es mehrere Minuten dauern kann, bis Security Hub CSPM Ihre Anfrage bearbeitet und das Ergebnis aktualisiert hat.

> **Tip**
>
> Sie können den Workflow-Status von Ergebnissen auch automatisch ändern, indem Sie Automatisierungsregeln verwenden. Mit Automatisierungsregeln konfigurieren Sie Security Hub CSPM so, dass der Workflow-Status von Ergebnissen auf der Grundlage der von Ihnen angegebenen Kriterien automatisch aktualisiert wird. Weitere Informationen finden Sie unter Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM.

Um den Workflow-Status eines oder mehrerer Ergebnisse zu ändern, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten.

Security Hub CSPM console

Um den Workflow-Status von Ergebnissen zu ändern

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus, um eine Tabelle mit Ergebnissen anzuzeigen:
   - Wählen Sie Ergebnisse aus.

- Wählen Sie Insights aus. Wählen Sie dann einen Einblick aus. Wählen Sie in den Insight-Ergebnissen ein Ergebnis aus.
- Wähle Sie Integrations (Integrationen) aus. Wählen Sie dann im Abschnitt für die Integration die Option Ergebnisse anzeigen aus.
- Wählen Sie Sicherheitsstandards aus. Wählen Sie dann im Abschnitt für den Standard die Option Ergebnisse anzeigen aus. Wählen Sie in der Kontrolltabelle ein Steuerelement aus, um die Ergebnisse für das Steuerelement anzuzeigen.

3. Aktivieren Sie in der Tabelle mit den Ergebnissen das Kontrollkästchen für jedes Ergebnis, dessen Workflow-Status Sie ändern möchten.
4. Wählen Sie oben auf der Seite Workflow-Status und dann den neuen Workflow-Status für die ausgewählten Ergebnisse aus.
5. Geben Sie im Dialogfeld Workflow-Status festlegen optional eine Notiz ein, in der der Grund für die Änderung des Workflow-Status detailliert beschrieben wird. Wählen Sie dann Status festlegen aus.

Security Hub CSPM API

Verwenden Sie die BatchUpdateFindingsOperation. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details mithilfe der GetFindingsOperation abrufen.

AWS CLI

Führen Sie den Befehl batch-update-findings aus. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details abrufen, indem Sie den Befehl get-findings ausführen.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Beispiel

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden

Sie können benutzerdefinierte AWS Security Hub CSPM-Aktionen erstellen, um Security Hub CSPM mit Amazon zu automatisieren. EventBridge Für benutzerdefinierte Aktionen lautet der Ereignistyp Security Hub Findings - Custom Action. Nachdem Sie eine benutzerdefinierte Aktion eingerichtet haben, können Sie Ergebnisse an sie senden. Weitere Informationen und detaillierte Schritte zum Erstellen benutzerdefinierter Aktionen finden Sie unter the section called “Automatisierte Reaktion und Problembehebung”.

Um Ergebnisse an eine benutzerdefinierte Aktion (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
   - Wählen Sie im Security Hub CSPM-Navigationsbereich Findings aus.
   - Wählen Sie im Security Hub CSPM-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
   - Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen, um eine Liste mit Kontrollen anzuzeigen. Wählen Sie dann den Namen des Steuerelements.
3. Aktivieren Sie in der Ergebnisliste das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.

   Sie können bis zu 20 Ergebnisse gleichzeitig senden.
4. Wählen Sie für Aktionen die benutzerdefinierte Aktion aus.

AWS Format für Sicherheitssuche (ASFF)

AWS Security Hub CSPM nutzt und aggregiert Erkenntnisse aus integrierten AWS-Services Produkten und Produkten von Drittanbietern. Security Hub CSPM verarbeitet diese Ergebnisse mithilfe eines Standardformats für Ergebnisse, dem AWS Security Finding Format (ASFF), das zeitaufwändige Datenkonvertierungen überflüssig macht.

Diese Seite bietet einen vollständigen Überblick über die JSON-Daten für ein Ergebnis im AWS Security Finding Format (ASFF). Das Format leitet sich vom JSON-Schema ab. Wählen Sie den Namen eines verknüpften Objekts, um ein Beispiel für ein Ergebnis für dieses Objekt zu überprüfen. Der Vergleich Ihrer Security Hub CSPM-Ergebnisse mit den hier aufgeführten Ressourcen und Beispielen kann Ihnen bei der Interpretation Ihrer Ergebnisse helfen.

Eine Beschreibung der einzelnen ASFF-Attribute finden Sie unter und. the section called “Erforderliche ASFF-Attribute der obersten Ebene” the section called “Optionale ASFF-Attribute der obersten Ebene”

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
```

```
        }
       },
       "ServiceName": "string"
      },
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
```

```
      "PortProbeDetails": [{
       "LocalIpDetails": {
        "IpAddressV4": "string"
       },
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "GeoLocation": {
         "Lat": number,
         "Lon": number
        },
        "IpAddressV4": "string",
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       }
      }]
     }
    },
    "AwsAccountId": "string",
    "AwsAccountName": "string",
    "CompanyName": "string",
    "Compliance": {
     "AssociatedStandards": [{
      "StandardsId": "string"
     }],
     "RelatedRequirements": ["string"],
     "SecurityControlId": "string",
     "SecurityControlParameters": [
      {
       "Name": "string",
       "Value": ["string"]
```

```
      }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
     "Detection": {
      "Sequence": {
       "Uid": "string",
       "Actors": [{
        "Id": "string",
        "Session": {
         "Uid": "string",
         "MfAStatus": "string",
         "CreatedTime": "string",
         "Issuer": "string"
        },
        "User": {
         "CredentialUid": "string",
         "Name": "string",
         "Type": "string",
         "Uid": "string",
         "Account": {
          "Uid": "string",
          "Name": "string"
         }
        }
       }],
       "Endpoints": [{
        "Id": "string",
        "Ip": "string",
        "Domain": "string",
        "Port": number,
        "Location": {
         "City": "string",
         "Country": "string",
```

```
          "Lat": number,
          "Lon": number
         },
         "AutonomousSystem": {
          "Name": "string",
          "Number": number
         },
         "Connection": {
          "Direction": "string"
         }
        }],
        "Signals": [{
         "Id": "string",
         "Title": "string",
         "ActorIds": ["string"],
         "Count": number,
         "FirstSeenAt": number,
         "SignalIndicators": [
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
          },
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
          }
         ],
         "LastSeenAt": number,
         "Name": "string",
         "ResourceIds": ["string"],
         "Type": "string"
        }],
        "SequenceIndicators": [
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
         },
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
```

```
        }
       ]
      }
     },
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
       "ProductArn": "string",
       "Id": "string"
      }],
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Types": ["string"]
     },
     "FirstObservedAt": "string",
     "GeneratorId": "string",
     "Id": "string",
     "LastObservedAt": "string",
     "Malware": [{
      "Name": "string",
      "Path": "string",
      "State": "string",
      "Type": "string"
     }],
     "Network": {
      "DestinationDomain": "string",
      "DestinationIpV4": "string",
      "DestinationIpV6": "string",
      "DestinationPort": number,
      "Direction": "string",
      "OpenPortRange": {
       "Begin": integer,
       "End": integer
      },
      "Protocol": "string",
      "SourceDomain": "string",
      "SourceIpV4": "string",
      "SourceIpV6": "string",
      "SourceMac": "string",
      "SourcePort": number
```

```
    },
    "NetworkPath": [{
     "ComponentId": "string",
     "ComponentType": "string",
     "Egress": {
      "Destination": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
      },
      "Protocol": "string",
      "Source": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
      }
     },
     "Ingress": {
      "Destination": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
      },
      "Protocol": "string",
      "Source": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
        "End": integer
       }]
      }
     }
    }],
    "Note": {
     "Text": "string",
     "UpdatedAt": "string",
     "UpdatedBy": "string"
    },
```

```
      "PatchSummary": {
       "FailedCount": number,
       "Id": "string",
       "InstalledCount": number,
       "InstalledOtherCount": number,
       "InstalledPendingReboot": number,
       "InstalledRejectedCount": number,
       "MissingCount": number,
       "Operation": "string",
       "OperationEndTime": "string",
       "OperationStartTime": "string",
       "RebootOption": "string"
      },
      "Process": {
       "LaunchedAt": "string",
       "Name": "string",
       "ParentPid": number,
       "Path": "string",
       "Pid": number,
       "TerminatedAt": "string"
      },
      "ProductArn": "string",
      "ProductFields": {
       "string": "string"
      },
      "ProductName": "string",
      "RecordState": "string",
      "Region": "string",
      "RelatedFindings": [{
       "Id": "string",
       "ProductArn": "string"
      }],
      "Remediation": {
       "Recommendation": {
        "Text": "string",
        "Url": "string"
       }
      },
      "Resources": [{
       "ApplicationArn": "string",
       "ApplicationName": "string",
       "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
```

```
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
         "Detections": [{
          "Arn": "string",
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
```

```
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
```

```
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
         "TimeOfDay": "string",
         "TimeZone": "string"
        },
        "PubliclyAccessible": boolean,
        "SecurityGroups": [
         "string"
        ],
        "StorageType": "string",
        "SubnetIds": [
         "string",
         "string"
        ],
```

```
        "Users": [{
         "Username": "string"
        }]
       },
       "AwsApiGatewayRestApi": {
        "ApiKeySource": "string",
        "BinaryMediaTypes": [" string"],
        "CreatedDate": "string",
        "Description": "string",
        "EndpointConfiguration": {
         "Types": ["string"]
        },
        "Id": "string",
        "MinimumCompressionSize": number,
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "CacheClusterEnabled": boolean,
        "CacheClusterSize": "string",
        "CacheClusterStatus": "string",
        "CanarySettings": {
         "DeploymentId": "string",
         "PercentTraffic": number,
         "StageVariableOverrides": [{
          "string": "string"
         }],
         "UseStageCache": boolean
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
```

```
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
         }],
         "StageName": "string",
         "TracingEnabled": boolean,
         "Variables": {
          "string": "string"
         },
         "WebAclArn": "string"
        },
        "AwsApiGatewayV2Api": {
         "ApiEndpoint": "string",
         "ApiId": "string",
         "ApiKeySelectionExpression": "string",
         "CorsConfiguration": {
          "AllowCredentials": boolean,
          "AllowHeaders": ["string"],
          "AllowMethods": ["string"],
          "AllowOrigins": ["string"],
          "ExposeHeaders": ["string"],
          "MaxAge": number
         },
         "CreatedDate": "string",
         "Description": "string",
         "Name": "string",
         "ProtocolType": "string",
         "RouteSelectionExpression": "string",
         "Version": "string"
        },
        "AwsApiGatewayV2Stage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "ApiGatewayManaged": boolean,
         "AutoDeploy": boolean,
         "ClientCertificateId": "string",
         "CreatedDate": "string",
```

```
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
         },
         {
          "AuthenticationType": "string"
         }
         ],
         "ApiId": "string",
         "Arn": "string",
         "AuthenticationType": "string",
         "Id": "string",
         "LogConfig": {
          "CloudWatchLogsRoleArn": "string",
          "ExcludeVerboseContent": boolean,
```

```
          "FieldLogLevel": "string"
         },
         "Name": "string",
         "XrayEnabled": boolean
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
        "Name": "string",
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "string",
          "LaunchTemplateName": "string",
          "Version": "string"
         },
         "CapacityRebalance": boolean,
         "Overrides": [{
          "InstanceType": "string",
          "WeightedCapacity": "string"
         }]
        }
       }
      },
      "AwsAutoScalingLaunchConfiguration": {
       "AssociatePublicIpAddress": boolean,
       "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
         "DeleteOnTermination": boolean,
         "Encrypted": boolean,
         "Iops": number,
         "SnapshotId": "string",
         "VolumeSize": number,
         "VolumeType": "string"
        },
        "NoDevice": boolean,
        "VirtualName": "string"
       }],
       "ClassicLinkVpcId": "string",
       "ClassicLinkVpcSecurityGroups": ["string"],
       "CreatedTime": "string",
       "EbsOptimized": boolean,
       "IamInstanceProfile": "string"
      },
      "ImageId": "string",
      "InstanceMonitoring": {
       "Enabled": boolean
      },
      "InstanceType": "string",
      "KernelId": "string",
      "KeyName": "string",
      "LaunchConfigurationName": "string",
      "MetadataOptions": {
       "HttpEndPoint": "string",
       "HttpPutReponseHopLimit": number,
```

```
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
         "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
         "CopyActions": [{
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
           "DeleteAfterDays": integer,
           "MoveToColdStorageAfterDays": integer
          }
         }],
         "Lifecycle": {
          "DeleteAfterDays": integer
         },
         "RuleName": "string",
         "ScheduleExpression": "string",
         "StartWindowMinutes": integer,
         "TargetBackupVault": "string"
        }]
       },
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "VersionId": "string"
      },
      "AwsBackupBackupVault": {
       "AccessPolicy": {
        "Statement": [{
         "Action": ["string"],
         "Effect": "string",
```

```
          "Principal": {
           "AWS": "string"
          },
          "Resource": "string"
         }],
         "Version": "string"
        },
        "BackupVaultArn": "string",
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
```

```
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
```

```
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "RenewalStatus": "string",
        "RenewalStatusReason": "string",
        "UpdatedAt": "string"
       },
       "Serial": "string",
       "SignatureAlgorithm": "string",
       "Status": "string",
       "Subject": "string",
       "SubjectAlternativeNames": ["string"],
       "Type": "string"
      },
      "AwsCloudFormationStack": {
       "Capabilities": ["string"],
       "CreationTime": "string",
       "Description": "string",
       "DisableRollback": boolean,
       "DriftInformation": {
        "StackDriftStatus": "string"
       },
       "EnableTerminationProtection": boolean,
       "LastUpdatedTime": "string",
       "NotificationArns": ["string"],
       "Outputs": [{
        "Description": "string",
        "OutputKey": "string",
        "OutputValue": "string"
       }],
       "RoleArn": "string",
       "StackId": "string",
       "StackName": "string",
       "StackStatus": "string",
       "StackStatusReason": "string",
       "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
       "CacheBehaviors": {
        "Items": [{
```

```
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
```

```
          }
         }]
        },
        "Status": "string",
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
         "CloudFrontDefaultCertificate": boolean,
         "IamCertificateId": "string",
         "MinimumProtocolVersion": "string",
         "SslSupportMethod": "string"
        },
        "WebAclId": "string"
       },
       "AwsCloudTrailTrail": {
        "CloudWatchLogsLogGroupArn": "string",
        "CloudWatchLogsRoleArn": "string",
        "HasCustomEventSelectors": boolean,
        "HomeRegion": "string",
        "IncludeGlobalServiceEvents": boolean,
        "IsMultiRegionTrail": boolean,
        "IsOrganizationTrail": boolean,
        "KmsKeyId": "string",
        "LogFileValidationEnabled": boolean,
        "Name": "string",
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
       },
       "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
         "Name": "string",
         "Value": "string"
```

```
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
      },
      "AwsCodeBuildProject": {
        "Artifacts": [{
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
          "Certificate": "string",
          "EnvironmentVariables": [{
            "Name": "string",
```

```
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
        }
       },
       "AwsDmsEndpoint": {
        "CertificateArn": "string",
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
```

```
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
      },
      "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
```

```
        }],
        "BillingModeSummary": {
         "BillingMode": "string",
         "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
         "Backfilling": boolean,
         "IndexArn": "string",
         "IndexName": "string",
         "IndexSizeBytes": number,
         "IndexStatus": "string",
         "ItemCount": number,
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
```

```
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        }
       }],
       "ProvisionedThroughput": {
        "LastDecreaseDateTime": "string",
        "LastIncreaseDateTime": "string",
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
       },
       "Replicas": [{
        "GlobalSecondaryIndexes": [{
         "IndexName": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         }
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
```

```
        "TableId": "string",
        "TableName": "string",
        "TableSizeBytes": number,
        "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
        "AuthenticationOptions": [
         {
          "MutualAuthentication": {
           "ClientRootCertificateChainArn": "string"
          },
          "Type": "string"
         }
        ],
        "ClientCidrBlock": "string",
        "ClientConnectOptions": {
         "Enabled": boolean
        },
        "ClientLoginBannerOptions": {
         "Enabled": boolean
        },
        "ClientVpnEndpointId": "string",
        "ConnectionLogOptions": {
         "Enabled": boolean
        },
        "Description": "string",
        "DnsServer": ["string"],
        "ServerCertificateArn": "string",
        "SecurityGroupIdSet": [
         "string"
        ],
        "SelfServicePortalUrl": "string",
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
      },
      "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
```

```
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
       },
       "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
         "HttpEndpoint": "string",
         "HttpProtocolIpv6": "string",
         "HttpPutResponseHopLimit": number,
         "HttpTokens": "string",
         "InstanceMetadataTags": "string"
        },
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
```

```
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         }
        }],
        "MetadataOptions": {
         "HttpTokens": "string",
         "HttpPutResponseHopLimit" : number
        },
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
```

```
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2NetworkInterface": {
        "Attachment": {
         "AttachmentId": "string",
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "DeviceIndex": number,
         "InstanceId": "string",
         "InstanceOwnerId": "string",
         "Status": "string"
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
         "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
         {
```

```
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         },
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
```

```
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
```

```
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
        "Attachments": [{
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "InstanceId": "string",
          "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlockState": "string",
          "Ipv6CidrBlock": "string"
        }],
        "State": "string"
      },
      "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
```

```
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
```

```
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
       },
       "RepositoryName": "string",
       "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
       "ActiveServicesCount": number,
       "CapacityProviders": ["string"],
       "ClusterArn": "string",
       "ClusterName": "string",
       "ClusterSettings": [{
        "Name": "string",
        "Value": "string"
       }],
       "Configuration": {
        "ExecuteCommandConfiguration": {
         "KmsKeyId": "string",
         "LogConfiguration": {
```

```
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
         },
         "Logging": "string"
        }
       },
       "DefaultCapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "RegisteredContainerInstancesCount": number,
       "RunningTasksCount": number,
       "Status": "string"
      },
      "AwsEcsContainer": {
       "Image": "string",
       "MountPoints": [{
        "ContainerPath": "string",
        "SourceVolume": "string"
       }],
       "Name": "string",
       "Privileged": boolean
      },
      "AwsEcsService": {
       "CapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "Cluster": "string",
       "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
         "Enable": boolean,
         "Rollback": boolean
        },
        "MaximumPercent": number,
        "MinimumHealthyPercent": number
       },
       "DeploymentController": {
        "Type": "string"
```

```
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
```

```
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
```

```
          "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
         "Hostname": "string",
         "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
```

```
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
         "CredentialsParameter": "string"
        },
        "ResourceRequirements": [{
         "Type": "string",
         "Value": "string"
        }],
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
```

```
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
         "VolumesFrom": [{
          "ReadOnly": boolean,
          "SourceContainer": "string"
         }],
         "WorkingDirectory": "string"
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
         "DeviceName": "string",
         "DeviceType": "string"
        }],
        "IpcMode": "string",
        "Memory": "string",
        "NetworkMode": "string",
        "PidMode": "string",
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "ProxyConfiguration": {
         "ContainerName": "string",
         "ProxyConfigurationProperties": [{
          "Name": "string",
          "Value": "string"
         }],
         "Type": "string"
        },
        "RequiresCompatibilities": ["string"],
        "Status": "string",
        "TaskRoleArn": "string",
        "Volumes": [{
         "DockerVolumeConfiguration": {
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
```

```
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
       },
       "AwsEfsAccessPoint": {
        "AccessPointId": "string",
        "Arn": "string",
        "ClientToken": "string",
        "FileSystemId": "string",
        "PosixUser": {
         "Gid": "string",
         "SecondaryGids": ["string"],
         "Uid": "string"
        },
        "RootDirectory": {
         "CreationInfo": {
          "OwnerGid": "string",
          "OwnerUid": "string",
          "Permissions": "string"
         },
         "Path": "string"
        }
       },
       "AwsEksCluster": {
        "Arn": "string",
        "CertificateAuthorityData": "string",
        "ClusterStatus": "string",
```

```
        "Endpoint": "string",
        "Logging": {
         "ClusterLogging": [{
          "Enabled": boolean,
          "Types": ["string"]
         }]
        },
        "Name": "string",
        "ResourcesVpcConfig": {
         "EndpointPublicAccess": boolean,
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "RoleArn": "string",
        "Version": "string"
       },
       "AwsElasticBeanstalkEnvironment": {
        "ApplicationName": "string",
        "Cname": "string",
        "DateCreated": "string",
        "DateUpdated": "string",
        "Description": "string",
        "EndpointUrl": "string",
        "EnvironmentArn": "string",
        "EnvironmentId": "string",
        "EnvironmentLinks": [{
         "EnvironmentName": "string",
         "LinkName": "string"
        }],
        "EnvironmentName": "string",
        "OptionSettings": [{
         "Namespace": "string",
         "OptionName": "string",
         "ResourceName": "string",
         "Value": "string"
        }],
        "PlatformArn": "string",
        "SolutionStackName": "string",
        "Status": "string",
        "Tier": {
         "Name": "string",
         "Type": "string",
         "Version": "string"
        },
```

```
        "VersionLabel": "string"
       },
       "AwsElasticSearchDomain": {
        "AccessPolicies": "string",
        "DomainStatus": {
         "DomainId": "string",
         "DomainName": "string",
         "Endpoint": "string",
         "Endpoints": {
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
```

```
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VPCOptions": {
        "AvailabilityZones": [
         "string"
        ],
        "SecurityGroupIds": [
         "string"
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
```

```
        "Instances": [{
         "InstanceId": "string"
        }],
        "ListenerDescriptions": [{
         "Listener": {
          "InstancePort": number,
          "InstanceProtocol": "string",
          "LoadBalancerPort": number,
          "Protocol": "string",
          "SslCertificateId": "string"
         },
         "PolicyNames": ["string"]
        }],
        "LoadBalancerAttributes": {
         "AccessLog": {
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                         "Key": "string",
                         "Value": "string"
                     }]
        },
        "LoadBalancerName": "string",
        "Policies": {
         "AppCookieStickinessPolicies": [{
          "CookieName": "string",
          "PolicyName": "string"
         }],
         "LbCookieStickinessPolicies": [{
          "CookieExpirationPeriod": number,
          "PolicyName": "string"
```

```
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
       "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
       "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
       "IpAddressType": "string",
       "LoadBalancerAttributes": [{
        "Key": "string",
        "Value": "string"
       }],
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "State": {
        "Code": "string",
        "Reason": "string"
       },
       "Type": "string",
       "VpcId": "string"
      },
      "AwsEventSchemasRegistry": {
       "Description": "string",
       "RegistryArn": "string",
       "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
       "Arn": "string",
       "Description": "string",
       "EndpointId": "string",
       "EndpointUrl": "string",
```

```
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
```

```
        "S3Logs": {
         "Status": "string"
        },
        "Kubernetes": {
         "AuditLogs": {
          "Status": "string"
         }
        },
        "MalwareProtection": {
         "ScanEc2InstanceWithFindings": {
          "EbsVolumes": {
           "Status": "string"
          }
         },
         "ServiceRole": "string"
        }
       }
      },
      "AwsIamAccessKey": {
       "AccessKeyId": "string",
       "AccountId": "string",
       "CreatedAt": "string",
       "PrincipalId": "string",
       "PrincipalName": "string",
       "PrincipalType": "string",
       "SessionContext": {
        "Attributes": {
         "CreationDate": "string",
         "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
         "AccountId": "string",
         "Arn": "string",
         "PrincipalId": "string",
         "Type": "string",
         "UserName": "string"
        }
       },
       "Status": "string"
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
```

```
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
```

```
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
```

```
      "AwsKmsKey": {
       "AWSAccountId": "string",
       "CreationDate": "string",
       "Description": "string",
       "KeyId": "string",
       "KeyManager": "string",
       "KeyRotationStatus": boolean,
       "KeyState": "string",
       "Origin": "string"
      },
      "AwsLambdaFunction": {
       "Architectures": [
        "string"
       ],
       "Code": {
        "S3Bucket": "string",
        "S3Key": "string",
        "S3ObjectVersion": "string",
        "ZipFile": "string"
       },
       "CodeSha256": "string",
       "DeadLetterConfig": {
        "TargetArn": "string"
       },
       "Environment": {
        "Variables": {
         "Stage": "string"
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
       "FunctionName": "string",
       "Handler": "string",
       "KmsKeyArn": "string",
       "LastModified": "string",
       "Layers": {
        "Arn": "string",
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
```

```
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
           "CertificateAuthorityArnList": [],
           "Enabled": boolean
          },
          "Unauthenticated": {
           "Enabled": boolean
          }
         },
         "ClusterName": "string",
         "CurrentVersion": "string",
         "EncryptionInfo": {
          "EncryptionAtRest": {
           "DataVolumeKMSKeyId": "string"
```

```
        },
        "EncryptionInTransit": {
         "ClientBroker": "string",
         "InCluster": boolean
        }
       },
       "EnhancedMonitoring": "string",
       "NumberOfBrokerNodes": integer
      }
     },
     "AwsNetworkFirewallFirewall": {
      "DeleteProtection": boolean,
      "Description": "string",
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [{
       "SubnetId": "string"
      }],
      "VpcId": "string"
     },
     "AwsNetworkFirewallFirewallPolicy": {
      "Description": "string",
      "FirewallPolicy": {
       "StatefulRuleGroupReferences": [{
        "ResourceArn": "string"
       }],
       "StatelessCustomActions": [{
        "ActionDefinition": {
         "PublishMetricAction": {
          "Dimensions": [{
           "Value": "string"
          }]
         }
        },
        "ActionName": "string"
       }],
       "StatelessDefaultActions": ["string"],
       "StatelessFragmentDefaultActions": ["string"],
       "StatelessRuleGroupReferences": [{
        "Priority": number,
```

```
          "ResourceArn": "string"
         }]
        },
        "FirewallPolicyArn": "string",
        "FirewallPolicyId": "string",
        "FirewallPolicyName": "string"
       },
       "AwsNetworkFirewallRuleGroup": {
        "Capacity": number,
        "Description": "string",
        "RuleGroup": {
         "RulesSource": {
          "RulesSourceList": {
           "GeneratedRulesType": "string",
           "Targets": ["string"],
           "TargetTypes": ["string"]
          },
          "RulesString": "string",
          "StatefulRules": [{
           "Action": "string",
           "Header": {
            "Destination": "string",
            "DestinationPort": "string",
            "Direction": "string",
            "Protocol": "string",
            "Source": "string",
            "SourcePort": "string"
           },
           "RuleOptions": [{
            "Keyword": "string",
            "Settings": ["string"]
           }]
          }],
          "StatelessRulesAndCustomActions": {
           "CustomActions": [{
            "ActionDefinition": {
             "PublishMetricAction": {
              "Dimensions": [{
               "Value": "string"
              }]
             }
            },
            "ActionName": "string"
           }],
```

```
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Sources": [{
              "AddressDefinition": "string"
             }],
             "TcpFlags": [{
              "Flags": ["string"],
              "Masks": ["string"]
             }]
            }
           }
          }]
         }
        },
        "RuleVariables": {
         "IpSets": {
          "Definition": ["string"]
         },
         "PortSets": {
          "Definition": ["string"]
         }
        }
       },
       "RuleGroupArn": "string",
       "RuleGroupId": "string",
       "RuleGroupName": "string",
       "Type": "string"
      },
      "AwsOpenSearchServiceDomain": {
```

```
        "AccessPolicies": "string",
        "AdvancedSecurityOptions": {
         "Enabled": boolean,
         "InternalUserDatabaseEnabled": boolean,
         "MasterUserOptions": {
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
```

```
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "OptionalDeployment": boolean,
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VpcOptions": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       }
      },
      "AwsRdsDbCluster": {
       "ActivityStreamStatus": "string",
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZones": ["string"],
       "BackupRetentionPeriod": integer,
       "ClusterCreateTime": "string",
       "CopyTagsToSnapshot": boolean,
       "CrossAccountClone": boolean,
```

```
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
```

```
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
```

```
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
```

```
        "Address": "string",
        "HostedZoneId": "string",
        "Port": number
      },
      "MasterUsername": "admin",
      "MaxAllocatedStorage": number,
      "MonitoringInterval": number,
      "MonitoringRoleArn": "string",
      "MultiAz": boolean,
      "OptionGroupMemberships": [{
        "OptionGroupName": "string",
        "Status": "string"
      }],
      "PendingModifiedValues": {
        "AllocatedStorage": number,
        "BackupRetentionPeriod": number,
        "CaCertificateIdentifier": "string",
        "DbInstanceClass": "string",
        "DbInstanceIdentifier": "string",
        "DbSubnetGroupName": "string",
        "EngineVersion": "string",
        "Iops": number,
        "LicenseModel": "string",
        "MasterUserPassword": "string",
        "MultiAZ": boolean,
        "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
        },
        "Port": number,
        "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
        }],
        "StorageType": "string"
      },
      "PerformanceInsightsEnabled": boolean,
      "PerformanceInsightsKmsKeyId": "string",
      "PerformanceInsightsRetentionPeriod": number,
      "PreferredBackupWindow": "string",
      "PreferredMaintenanceWindow": "string",
      "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
```

```
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
         "CidrIp": "string",
         "Status": "string"
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsRdsDbSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZone": "string",
        "DbInstanceIdentifier": "string",
        "DbiResourceId": "string",
        "DbSnapshotIdentifier": "string",
```

```
        "Encrypted": boolean,
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
```

```
        "PrivateIPAddress": "string",
        "PublicIPAddress": "string"
      }],
      "ClusterParameterGroups": [{
        "ClusterParameterStatusList": [{
          "ParameterApplyErrorDescription": "string",
          "ParameterApplyStatus": "string",
          "ParameterName": "string"
        }],
        "ParameterApplyStatus": "string",
        "ParameterGroupName": "string"
      }],
      "ClusterPublicKey": "string",
      "ClusterRevisionNumber": "string",
      "ClusterSecurityGroups": [{
        "ClusterSecurityGroupName": "string",
        "Status": "string"
      }],
      "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "string",
        "ManualSnapshotRetentionPeriod": number,
        "RetentionPeriod": number,
        "SnapshotCopyGrantName": "string"
      },
      "ClusterStatus": "string",
      "ClusterSubnetGroupName": "string",
      "ClusterVersion": "string",
      "DBName": "string",
      "DeferredMaintenanceWindows": [{
        "DeferMaintenanceEndTime": "string",
        "DeferMaintenanceIdentifier": "string",
        "DeferMaintenanceStartTime": "string"
      }],
      "ElasticIpStatus": {
        "ElasticIp": "string",
        "Status": "string"
      },
      "ElasticResizeNumberOfNodeOptions": "string",
      "Encrypted": boolean,
      "Endpoint": {
        "Address": "string",
        "Port": number
      },
      "EnhancedVpcRouting": boolean,
```

```
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
```

```
        "ResizeType": "string"
       },
       "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": number,
        "ElapsedTimeInSeconds": number,
        "EstimatedTimeToCompletionInSeconds": number,
        "ProgressInMegaBytes": number,
        "SnapshotSizeInMegaBytes": number,
        "Status": "string"
       },
       "SnapshotScheduleIdentifier": "string",
       "SnapshotScheduleState": "string",
       "VpcId": "string",
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRoute53HostedZone": {
       "HostedZone": {
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
        }
       },
       "Vpcs": [
        {
         "Id": "string",
         "Region": "string"
        }
       ]
      },
      "AwsS3AccessPoint": {
       "AccessPointArn": "string",
       "Alias": "string",
```

```
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
               "Value": "string"
              },
              "Type": "string"
             }
            ],
```

```
          "Type": "string"
         }
        },
        "Id": "string",
        "NoncurrentVersionExpirationInDays": number,
        "NoncurrentVersionTransitions": [{
         "Days": number,
         "StorageClass": "string"
        }],
        "Prefix": "string",
        "Status": "string",
        "Transitions": [{
         "Date": "string",
         "Days": number,
         "StorageClass": "string"
        }]
       }]
      },
      "BucketLoggingConfiguration": {
       "DestinationBucketName": "string",
       "LogFilePrefix": "string"
      },
      "BucketName": "string",
      "BucketNotificationConfiguration": {
       "Configurations": [{
        "Destination": "string",
        "Events": ["string"],
        "Filter": {
         "S3KeyFilter": {
          "FilterRules": [{
           "Name": "string",
           "Value": "string"
          }]
         }
        },
        "Type": "string"
       }]
      },
      "BucketVersioningConfiguration": {
       "IsMfaDeleteEnabled": boolean,
       "Status": "string"
      },
      "BucketWebsiteConfiguration": {
       "ErrorDocument": "string",
```

```
        "IndexDocumentSuffix": "string",
        "RedirectAllRequestsTo": {
         "HostName": "string",
         "Protocol": "string"
        },
        "RoutingRules": [{
         "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
         },
         "Redirect": {
          "HostName": "string",
          "HttpRedirectCode": "string",
          "Protocol": "string",
          "ReplaceKeyPrefixWith": "string",
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
       "ObjectLockConfiguration": {
        "ObjectLockEnabled": "string",
        "Rule": {
         "DefaultRetention": {
          "Days": integer,
          "Mode": "string",
          "Years": integer
         }
        }
       },
       "OwnerAccountId": "string",
       "OwnerId": "string",
       "OwnerName": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "ServerSideEncryptionConfiguration": {
        "Rules": [{
         "ApplyServerSideEncryptionByDefault": {
          "KMSMasterKeyID": "string",
          "SSEAlgorithm": "string"
```

```
        }
       }]
      }
     },
     "AwsS3Object": {
      "ContentType": "string",
      "ETag": "string",
      "LastModified": "string",
      "ServerSideEncryption": "string",
      "SSEKMSKeyId": "string",
      "VersionId": "string"
     },
     "AwsSagemakerNotebookInstance": {
      "DirectInternetAccess": "string",
      "InstanceMetadataServiceConfiguration": {
       "MinimumInstanceMetadataServiceVersion": "string"
      },
      "InstanceType": "string",
      "LastModifiedTime": "string",
      "NetworkInterfaceId": "string",
      "NotebookInstanceArn": "string",
      "NotebookInstanceName": "string",
      "NotebookInstanceStatus": "string",
      "PlatformIdentifier": "string",
      "RoleArn": "string",
      "RootAccess": "string",
      "SecurityGroups": ["string"],
      "SubnetId": "string",
      "Url": "string",
      "VolumeSizeInGB": number
     },
     "AwsSecretsManagerSecret": {
      "Deleted": boolean,
      "Description": "string",
      "KmsKeyId": "string",
      "Name": "string",
      "RotationEnabled": boolean,
      "RotationLambdaArn": "string",
      "RotationOccurredWithinFrequency": boolean,
      "RotationRules": {
       "AutomaticallyAfterDays": integer
      }
     },
     "AwsSnsTopic": {
```

```
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
```

```
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRule": {
       "MetricName": "string",
       "Name": "string",
       "RuleId": "string",
       "PredicateList": [{
```

```
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
         }]
        },
        "AwsWafRegionalRuleGroup": {
         "MetricName": "string",
         "Name": "string",
         "RuleGroupId": "string",
         "Rules": [{
          "Action": {
           "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string"
         }]
        },
        "AwsWafRegionalWebAcl": {
         "DefaultAction": "string",
         "MetricName" : "string",
         "Name": "string",
         "RulesList" : [{
          "Action": {
           "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string",
          "ExcludedRules": [{
           "ExclusionType": "string",
           "RuleId": "string"
          }],
          "OverrideAction": {
           "Type": "string"
          }
         }],
         "WebAclId": "string"
        },
        "AwsWafRule": {
         "MetricName": "string",
         "Name": "string",
         "PredicateList": [{
          "DataId": "string",
```

```
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "Awswafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
```

```
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string",
          "SampledRequestsEnabled": boolean
         }
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }],
        "WebAclId": "string"
       },
       "AwsWafv2WebAcl": {
        "Arn": "string",
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
```

```
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "CodeRepository": {
        "CodeSecurityIntegrationArn": "string",
        "ProjectName": "string",
        "ProviderType": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
```

```
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
```

```
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
         "StartLine": integer
        },
        "SourceArn":"string"
       }],
       "Cvss": [{
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
```

```
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte

AWS Security Hub CSPM bietet zwei Arten der Konsolidierung von Kontrollen:

- Ansicht konsolidierter Kontrollen — Bei dieser Art der Konsolidierung hat jede Kontrolle für alle Standards eine einzige Kennung. Darüber hinaus werden auf der Security Hub CSPM-Konsole auf der Seite „Kontrollen“ alle Kontrollen für alle Standards angezeigt.
- Konsolidierte Kontrollergebnisse — Bei dieser Art der Konsolidierung liefert Security Hub CSPM ein einziges Ergebnis für eine Kontrolle, auch wenn die Kontrolle für mehrere aktivierte Standards gilt. Dadurch kann das Suchgeräusch reduziert werden.

Sie können die Ansicht der konsolidierten Steuerelemente nicht aktivieren oder deaktivieren. Consolidated Control Findings ist standardmäßig aktiviert, wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren. Andernfalls ist es standardmäßig deaktiviert. Für Unternehmen ist Consolidated Control Findings jedoch nur für Security Hub CSPM-Mitgliedskonten aktiviert, wenn sie für das Administratorkonto aktiviert sind. Weitere Informationen zu konsolidierten Kontrollergebnissen finden Sie unter. Generierung und Aktualisierung von Kontrollergebnissen

Beide Konsolidierungsarten wirken sich auf Felder und Werte für Kontrollergebnisse in der ausAWS Format für Sicherheitssuche (ASFF).

Themen

- Ansicht konsolidierter Kontrollen — ASFF-Änderungen
- Konsolidierte Kontrollergebnisse — ASFF-Änderungen

- Generator-IDs vor und nach der Aktivierung konsolidierter Kontrollergebnisse
- Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt
- Aktualisierung der Workflows für die Konsolidierung

Ansicht konsolidierter Kontrollen — ASFF-Änderungen

Mit der Funktion zur Ansicht konsolidierter Kontrollen wurden die folgenden Änderungen an Feldern und Werten für Kontrollergebnisse in der ASFF eingeführt. Wenn Ihre Workflows nicht auf Werten für diese ASFF-Felder basieren, sind keine Maßnahmen erforderlich. Wenn Sie Workflows haben, die auf bestimmten Werten für diese Felder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen und Beschreibung der Änderung
Compliance.SecurityControlId	Nicht zutreffend (neues Feld)	EC2.2 Führt eine einzige Kontroll-ID für alle Standards ein. `ProductFields.RuleId` bietet immer noch die standardbasierte Kontroll-ID für CIS v1.2.0-Steuereleme nte. `ProductFields.ControlId` stellt immer noch die standardbasierte Kontroll-ID für Steuerungen in anderen Standards bereit.
Compliance.AssociatedStandards	Nicht zutreffend (neues Feld)	[{“ StandardsId „:" standards /aws -foundational-security-best- /1.0.0 „}] practices/v Zeigt an, in welchen Standards ein Steuerelement aktiviert ist.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen und Beschreibung der Änderung
ProductFields.ArchivalReasons:0/Description	Nicht zutreffend (neues Feld)	„Das Ergebnis befindet sich im Status ARCHIVIERT, da konsolidierte Kontrolle rgebnisse aktiviert oder deaktiviert wurden. Dies führt dazu, dass Ergebnisse im vorherigen Status archiviert werden, wenn neue Ergebniss e generiert werden.“ Beschreibt, warum Security Hub CSPM bestehende Ergebnisse archiviert hat.
ProductFields.ArchivalReasons:0/ReasonCode	Nicht zutreffend (neues Feld)	„CONSOLIDATED_CONTROL_FINDINGS_UPDATE“ Liefert den Grund, warum Security Hub CSPM bestehende Ergebnisse archiviert hat.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen und Beschreibung der Änderung
Remediation.Recommendation.Text	„Anweisungen zur Behebung dieses Problems finden Sie in der AWS Security Hub CSPM PCI DSS-Dokumentation.“	„Anweisungen zur Behebung dieses Problems finden Sie in der Dokumentation zu den CSPM-Steuerungen von AWS Security Hub.“ Dieses Feld verweist nicht mehr auf einen Standard.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.

Konsolidierte Kontrollergebnisse — ASFF-Änderungen

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, sind Sie möglicherweise von den folgenden Änderungen an Feldern und Werten für Kontrollergebnisse im ASFF betroffen. Diese Änderungen kommen zu den Änderungen hinzu, die durch die Funktion zur Ansicht konsolidierter Kontrollen eingeführt wurden. Wenn Ihre Workflows nicht auf Werten für diese ASFF-Felder basieren, sind keine Maßnahmen erforderlich. Wenn Sie Workflows haben, die auf bestimmten Werten für diese Felder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

> **Tip**
>
> Wenn Sie die Lösung Automated Security Response auf AWS Version 2.0.0 verwenden, beachten Sie, dass sie konsolidierte Kontrollergebnisse unterstützt. Das bedeutet, dass Sie Ihre aktuellen Workflows beibehalten können, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
GeneratorId	aws-foundational-security-best- /1.0. practices/v 0/Config1.	Sicherheit- control/Config 1. Dieses Feld verweist nicht mehr auf einen Standard.
Title	PCI.Config.1 AWS Config sollte aktiviert sein	AWS Config sollte aktiviert sein Dieses Feld verweist nicht mehr auf standardspezifische Informationen.
Id	arn:aws:securityhub:eu-central-1:123456789012: - /3.2. subscription/pci dss/v 1/PCI. IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:security-. control/iam 9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Dieses Feld verweist nicht mehr auf einen Standard.
ProductFields.ControlId	PCI.EC2.2	Entfernt. Siehe `Compliance.SecurityControlId` stattdessen. Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.
ProductFields.RuleId	1.3	Entfernt. Siehe `Compliance.SecurityControlId` stattdessen. Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
Description	Diese PCI-DSS-Steuerung prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist.	Diese AWS Kontrolle prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist. Dieses Feld verweist nicht mehr auf einen Standard.

Schweregrad	„Schweregrad“: {
	
	„Produkt“: 90,
	
	„Label“: „KRITISCH“,
	
	„Normalisiert“: 90,
	
	„Original“: „KRITISCH“
	
	}
		„Schweregrad“: {
		
		„Label“: „KRITISCH“,
		
		„Normalisiert“: 90,
		
		„Original“: „KRITISCH“
		
		}
		
		Security Hub CSPM verwendet das Feld Produkt nicht mehr, um den Schweregrad eines Fehlers zu beschreiben.

Typen	["Software und Konfiguration Checks/Industry und gesetzliche Vorschriften Standards/PCI-DSS „]	["Software und Konfiguration Checks/Industry sowie regulator ische Standards"] Dieses Feld verweist nicht mehr auf einen Standard.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
Compliance.Related Requirements	["PCI DSS 10.5.2“, „PCI DSS 11.5", „CIS AWS Foundations 2.5"]	["PCI DSS v3.2. 1/105,2 Zoll, „PCI DSS v3.2. 1/113,5 Zoll, „Benchmark v1.2 AWS für CIS Foundations. 0/2.5"] In diesem Feld werden die entsprechenden Anforderungen für alle aktivierten Standards angezeigt.
CreatedAt	05.05.2022 T08:18:13.138Z	25.09.2022 T08:18:13.138Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie konsolidierte Kontrolle rgebnisse aktivieren.
FirstObservedAt	07.05.2022 T08:18:13.138Z	28.09.2022 T08:18:13.138Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie konsolidierte Kontrolle rgebnisse aktivieren.
ProductFields.Recommendation Url	https://docs.aws.amazon.com /console/securityhub/EC2.2/ remediation	Entfernt. Siehe `Remediation.Recommendation.Url` stattdessen.
ProductFields.StandardsArn	arn:aws:securityhub::: -foundational-security-best- /1.0.0 standards/aws practices/v	Entfernt. Siehe `Compliance.AssociatedStandards` stattdessen.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0. control/aws practices/v 0/Config1.	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.StandardsGuideArn	arn:aws:securityhub::: -aws-foundations- /1.2.0 ruleset/cis benchmark/v	Entfernt. Siehe `Compliance.AssociatedStandards` stattdessen.
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east- 2:123456789012: -aws-foundations- /1.2.0 subscription/cis benchmark/v	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0.0 subscription/aws practices/v	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east -1:: /:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0. product/aws securityhub/arn subscription/aws practices/v 0/Config. 1/finding /751c2173-7372-4e12-8656-a5210dfb1d67	arn:aws:securityhub:us-east -1:: /:aws:securityhub:us-east-1:123456789012:sicherheit-. product/aws securityhub/arn control/Config 1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Dieses Feld verweist nicht mehr auf einen Standard.

Werte für vom Kunden bereitgestellte ASFF-Felder nach Aktivierung der konsolidierten Kontrollergebnisse

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub CSPM ein standardübergreifendes Ergebnis und archiviert die ursprünglichen Ergebnisse (separate Ergebnisse für jeden Standard).

Aktualisierungen, die Sie mit der Security Hub CSPM-Konsole oder dem BatchUpdateFindingsVorgang an den ursprünglichen Ergebnissen vorgenommen haben, werden in den neuen Ergebnissen nicht beibehalten. Bei Bedarf können Sie diese Daten wiederherstellen, indem Sie auf die archivierten Ergebnisse zurückgreifen. Um archivierte Ergebnisse zu überprüfen, können Sie die Seite Ergebnisse in der Security Hub CSPM-Konsole verwenden und den Filter Datensatzstatus auf ARCHIVIERT setzen. Alternativ können Sie den GetFindingsBetrieb der Security Hub CSPM-API verwenden.

Customer-provided ASFF-Feld	Beschreibung der Änderung nach der Aktivierung der konsolidierten Kontrollergebnisse
Wahrscheinlichkeit	Setzt auf den leeren Zustand zurück.
Kritikalität	Setzt auf den leeren Zustand zurück.
Hinweis	Setzt auf den leeren Zustand zurück.
RelatedFindings	Setzt auf den leeren Zustand zurück.
Schweregrad	Standardschweregrad des Ergebnisses (entspricht dem Schweregrad der Kontrolle).
Typen	Wird auf den standardunabhängigen Wert zurückgesetzt.
UserDefinedFields	Setzt auf den leeren Zustand zurück.
VerificationState	Setzt auf den leeren Zustand zurück.
Workflow	Neue fehlgeschlagene Ergebnisse haben den Standardwert. `NEW` Neue bestandene Ergebnisse haben einen Standardwert von`RESOLVED`.

Generator-IDs vor und nach der Aktivierung konsolidierter Kontrollergebnisse

In der folgenden Tabelle sind Änderungen an den Generator-ID-Werten für Kontrollen aufgeführt, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Diese Änderungen gelten für Kontrollen, die Security Hub CSPM am 15. Februar 2023 unterstützt hat.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.1	Sicherheit- 1. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.10	Sicherheit- 1.6 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.11	Sicherheit- 1.7 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.12	Sicherheit- 4. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.13	Sicherheit- 9. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.14	Sicherheit- 6. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.16	Sicherheit- 1.2 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.2	Sicherheit- 5. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1,20	Sicherheit- 1.8 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.22	Sicherheit- 1. control/IAM

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.3	Sicherheit- 8. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.4	Sicherheit- 3. control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.5	Sicherheit- 1.1 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.6	Sicherheit- 1.2 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.7	Sicherheit- 1.3 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.8	Sicherheit- 1.4 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/1.9	Sicherheit- 1.5 control/IAM
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.1	Sicherheit- 1. control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.2	Sicherheit- 4. control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.3	Sicherheit- 6. control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.4	Sicherheit- 5. control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.5	Sicherheit- 1. control/Config

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.6	Sicherheit- 7. control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.7	Sicherheit- .2 control/CloudTrail
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.8	Sicherheit- 4. control/KMS
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/2.9	Sicherheit- 6. control/EC2
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.1	Sicherheit- 2.2 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.2	Sicherheit- 3. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.3	Sicherheit- 1. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.4	Sicherheit- 4. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.5	Sicherheit- 5. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.6	Sicherheit- .6 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.7	Sicherheit- 7. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.8	Sicherheit- 8. control/CloudWatch

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.9	Sicherheit- 9. control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.10	Sicherheit- 1.0 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.11	Sicherheit- 1.1 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.12	Sicherheit- 1.2 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.13	Sicherheit- 1.3 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/3.14	Sicherheit- 1.4 control/CloudWatch
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4.1	Sicherheit- 1.3 control/EC2
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4.2	Sicherheit- 1.4 control/EC2
arn:aws:securityhub::: -aws-foundations- /1.2. ruleset/cis benchmark/v 0/rule/4.3	Sicherheit- .2 control/EC2
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.10	Sicherheit- 5. control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.14	Sicherheit- 3. control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.16	Sicherheit- 1. control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.17	Sicherheit- 1.8 control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.4	Sicherheit- 4. control/IAM

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
cis-aws-Stiftungen- /1.4. benchmark/v 0/15.	Sicherheit- 9. control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.6	Sicherheit- 6. control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/17.	Sicherheit- 1. control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/1.8	Sicherheit- 1.5 control/IAM
cis-aws-Stiftungen- /1.4. benchmark/v 0/19.	Sicherheit- 1.6 control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/21.1.2	Sicherheit- .5 control/S3
cis-aws-Stiftungen- /1.4. benchmark/v 0/21.1.5. 1	Sicherheit- 1. control/S3
cis-aws-Stiftungen- /1.4. benchmark/v 0/21.1.5. 2	Sicherheit- .8 control/S3
cis-aws-Stiftungen- /1.4. benchmark/v 0/2.2.1	Sicherheit- 7. control/EC2
cis-aws-Stiftungen- /1.4. benchmark/v 0/23.3.1	Sicherheit- 3. control/RDS
cis-aws-Stiftungen- /1.4. benchmark/v 0/31.	Sicherheit- control/CloudTrail 1.
cis-aws-Stiftungen- /1.4. benchmark/v 0/31.2	Sicherheit- control/CloudTrail 4.
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.4	Sicherheit- 5. control/CloudTrail
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.5	Sicherheit- 1. control/Config
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.6	Sicherheit- 9. control/S3
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.7	Sicherheit- 2. control/CloudTrail
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.8	Sicherheit- 4. control/KMS
cis-aws-Stiftungen- /1.4. benchmark/v 0/3.9	Sicherheit- 6. control/EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
cis-aws-Stiftungen- /1.4. benchmark/v 0/43.	Sicherheit- control/CloudWatch 1.
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.4	Sicherheit- 4. control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.5	Sicherheit- 5. control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.6	Sicherheit- 6. control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.7	Sicherheit- 7. control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.8	Sicherheit- 8. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/4.9	Sicherheit- 9. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/4.10	Sicherheit- 1.0 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/4.11	Sicherheit- 1.1 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.2	Sicherheit- 1.2 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.3	Sicherheit- 1.3 control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/4.14	Sicherheit- 1.4 control/CloudWatch
cis-aws-Stiftungen- /1.4. benchmark/v 0/51.	Sicherheit- control/EC2 2.1
cis-aws-Stiftungen- /1.4. benchmark/v 0/53.	Sicherheit- control/EC2 2.
aws-fundamentale-security-best- /1.0. practices /v 0/Account1.	Sicherheit- control/Account 1.
aws-fundamentale-security-best- /1.0. practices /v 0/ACM1.	Sicherheit- control/ACM 1.
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway1.	Sicherheit- control/APIGateway 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway.2	Sicherheit- control/APIGateway .2
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway3.	Sicherheit- control/APIGateway 3.
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway.4	Sicherheit- 4. control/APIGateway
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway.5	Sicherheit- 5. control/APIGateway
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway.8	Sicherheit- 8. control/APIGateway
aws-fundamentale-security-best- /1.0. practices /v 0/APIGateway.9	Sicherheit- 9. control/APIGateway
aws-fundamentale-security-best- /1.0. practices /v 0/AutoScaling1.	Sicherheit- control/AutoScaling 1.
aws-fundamentale-security-best- /1.0. practices /v 0/AutoScaling.2	Sicherheit- control/AutoScaling .2
aws-fundamentale-security-best- /1.0. practices /v 0/AutoScaling3.	Sicherheit- control/AutoScaling 3.
aws-fundamentale-security-best- /1.0. practices /v 0/Autoscaling.5	Sicherheit- 5. control/Autoscaling
aws-fundamentale-security-best- /1.0. practices /v 0/AutoScaling.6	Sicherheit- 6. control/AutoScaling
aws-fundamentale-security-best- /1.0. practices /v 0/AutoScaling.9	Sicherheit- 9. control/AutoScaling

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront1.	Sicherheit- control/CloudFront 1.
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront3.	Sicherheit- control/CloudFront 3.
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.4	Sicherheit- 4. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.5	Sicherheit- 5. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.6	Sicherheit- 6. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.7	Sicherheit- 7. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.8	Sicherheit- 8. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.9	Sicherheit- 9. control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.10	Sicherheit- 1.0 control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudFront.12	Sicherheit- 1.2 control/CloudFront
aws-fundamentale-security-best- /1.0. practices /v 0/CloudTrail1.	Sicherheit- control/CloudTrail 1.
aws-fundamentale-security-best- /1.0. practices /v 0/CloudTrail.2	Sicherheit- control/CloudTrail .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/CloudTrail.4	Sicherheit- 4. control/CloudTrail
aws-fundamentale-security-best- /1.0. practices /v 0/CloudTrail.5	Sicherheit- 5. control/CloudTrail
aws-fundamentale-security-best- /1.0. practices /v 0/CodeBuild1.	Sicherheit- control/CodeBuild 1.
aws-fundamentale-security-best- /1.0. practices /v 0/CodeBuild.2	Sicherheit- control/CodeBuild .2
aws-fundamentale-security-best- /1.0. practices /v 0/CodeBuild3.	Sicherheit- control/CodeBuild 3.
aws-fundamentale-security-best- /1.0. practices /v 0/CodeBuild.4	Sicherheit- 4. control/CodeBuild
aws-fundamentale-security-best- /1.0. practices /v 0/Config1.	Sicherheit- control/Config 1.
aws-fundamentale-security-best- /1.0. practices /v 0/DMS1.	Sicherheit- control/DMS 1.
aws-fundamentale-security-best- /1.0. practices /v 0/DynamoDB1.	Sicherheit- control/DynamoDB 1.
aws-fundamentale-security-best- /1.0. practices /v 0/DynamoDB.2	Sicherheit- control/DynamoDB .2
aws-fundamentale-security-best- /1.0. practices /v 0/DynamoDB3.	Sicherheit- control/DynamoDB 3.
aws-fundamentale-security-best- /1.0. practices /v 0/EC21.	Sicherheit- control/EC2 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/EC23.	Sicherheit- control/EC2 3.
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.4	Sicherheit- 4. control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.6	Sicherheit- 6. control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.7	Sicherheit- 7. control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.8	Sicherheit- 8. control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.9	Sicherheit- 9. control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.10	Sicherheit- 1.0 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.15	Sicherheit- 1.5 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.16	Sicherheit- 1.6 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.17	Sicherheit- 1.7 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.18	Sicherheit- 1.8 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.19	Sicherheit- 1.9 control/EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.2	Sicherheit- control/EC2 .2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.20	Sicherheit- 2.0 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.21	Sicherheit- 2.1 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.23	Sicherheit- 2.3 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.24	Sicherheit- 2.4 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/EC2.25	Sicherheit- 2.5 control/EC2
aws-fundamentale-security-best- /1.0. practices /v 0/ECR1.	Sicherheit- control/ECR 1.
aws-fundamentale-security-best- /1.0. practices /v 0/ECR.2	Sicherheit- control/ECR .2
aws-fundamentale-security-best- /1.0. practices /v 0/ECR3.	Sicherheit- control/ECR 3.
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.10	Sicherheit- 1.0 control/ECS
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.12	Sicherheit- 1.2 control/ECS
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.2	Sicherheit- control/ECS .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/ECS3.	Sicherheit- control/ECS 3.
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.4	Sicherheit- 4. control/ECS
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.5	Sicherheit- 5. control/ECS
aws-fundamentale-security-best- /1.0. practices /v 0/ECS.8	Sicherheit- 8. control/ECS
aws-fundamentale-security-best- /1.0. practices /v 0/EFS1.	Sicherheit- control/EFS 1.
aws-fundamentale-security-best- /1.0. practices /v 0/EFS.2	Sicherheit- control/EFS .2
aws-fundamentale-security-best- /1.0. practices /v 0/EFS3.	Sicherheit- control/EFS 3.
aws-fundamentale-security-best- /1.0. practices /v 0/EFS.4	Sicherheit- 4. control/EFS
aws-fundamentale-security-best- /1.0. practices /v 0/EKS.2	Sicherheit- control/EKS .2
aws-fundamentale-security-best- /1.0. practices /v 0/ElasticBeanstalk1.	Sicherheit- control/ElasticBeanstalk 1.
aws-fundamentale-security-best- /1.0. practices /v 0/ElasticBeanstalk.2	Sicherheit- control/ElasticBeanstalk .2
aws-fundamentale-security-best- /1.0. practices /v 0/ELBv21.	Sicherheit- control/ELB 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.2	Sicherheit- control/ELB .2
aws-fundamentale-security-best- /1.0. practices /v 0/ELB3.	Sicherheit- control/ELB 3.
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.4	Sicherheit- 4. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.5	Sicherheit- 5. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.6	Sicherheit- 6. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.7	Sicherheit- 7. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.8	Sicherheit- 8. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.9	Sicherheit- 9. control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.10	Sicherheit- 1.0 control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.11	Sicherheit- 1.1 control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.12	Sicherheit- 1.2 control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.13	Sicherheit- 1.3 control/ELB

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/ELB.14	Sicherheit- 1.4 control/ELB
aws-fundamentale-security-best- /1.0. practices /v 0/EMR1.	Sicherheit- control/EMR 1.
aws-fundamentale-security-best- /1.0. practices /v 0/ES1.	Sicherheit- control/ES 1.
aws-fundamentale-security-best- /1.0. practices /v 0/ES.2	Sicherheit- control/ES .2
aws-fundamentale-security-best- /1.0. practices /v 0/ES3.	Sicherheit- control/ES 3.
aws-fundamentale-security-best- /1.0. practices /v 0/ES.4	Sicherheit- 4. control/ES
aws-fundamentale-security-best- /1.0. practices /v 0/ES.5	Sicherheit- 5. control/ES
aws-fundamentale-security-best- /1.0. practices /v 0/ES.6	Sicherheit- 6. control/ES
aws-fundamentale-security-best- /1.0. practices /v 0/ES.7	Sicherheit- 7. control/ES
aws-fundamentale-security-best- /1.0. practices /v 0/ES.8	Sicherheit- 8. control/ES
aws-fundamentale-security-best- /1.0. practices /v 0/GuardDuty1.	Sicherheit- control/GuardDuty 1.
aws-fundamentale-security-best- /1.0. practices /v 0/IAM1.	Sicherheit- control/IAM 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.2	Sicherheit- control/IAM .2
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.21	Sicherheit- 2.1 control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/IAM3.	Sicherheit- control/IAM 3.
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.4	Sicherheit- 4. control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.5	Sicherheit- 5. control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.6	Sicherheit- 6. control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.7	Sicherheit- 7. control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/IAM.8	Sicherheit- 8. control/IAM
aws-fundamentale-security-best- /1.0. practices /v 0/Kinesis1.	Sicherheit- control/Kinesis 1.
aws-fundamentale-security-best- /1.0. practices /v 0/KMS1.	Sicherheit- control/KMS 1.
aws-fundamentale-security-best- /1.0. practices /v 0/KMS.2	Sicherheit- control/KMS .2
aws-fundamentale-security-best- /1.0. practices /v 0/KMS3.	Sicherheit- control/KMS 3.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/Lambda1.	Sicherheit- control/Lambda 1.
aws-fundamentale-security-best- /1.0. practices /v 0/Lambda.2	Sicherheit- control/Lambda .2
aws-fundamentale-security-best- /1.0. practices /v 0/Lambda.5	Sicherheit- 5. control/Lambda
aws-fundamentale-security-best- /1.0. practices /v 0/NetworkFirewall3.	Sicherheit- control/NetworkFirewall 3.
aws-fundamentale-security-best- /1.0. practices /v 0/NetworkFirewall.4	Sicherheit- 4. control/NetworkFirewall
aws-fundamentale-security-best- /1.0. practices /v 0/NetworkFirewall.5	Sicherheit- 5. control/NetworkFirewall
aws-fundamentale-security-best- /1.0. practices /v 0/NetworkFirewall.6	Sicherheit- 6. control/NetworkFirewall
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch1.	Sicherheit- control/Opensearch 1.
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.2	Sicherheit- control/Opensearch .2
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch3.	Sicherheit- control/Opensearch 3.
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.4	Sicherheit- 4. control/Opensearch
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.5	Sicherheit- 5. control/Opensearch

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.6	Sicherheit- 6. control/Opensearch
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.7	Sicherheit- 7. control/Opensearch
aws-fundamentale-security-best- /1.0. practices /v 0/Opensearch.8	Sicherheit- 8. control/Opensearch
aws-fundamentale-security-best- /1.0. practices /v 0/RDS1.	Sicherheit- control/RDS 1.
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.10	Sicherheit- 1.0 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.11	Sicherheit- 1.1 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.12	Sicherheit- 1.2 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.13	Sicherheit- 1.3 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.14	Sicherheit- 1.4 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.15	Sicherheit- 1.5 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.16	Sicherheit- 1.6 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.17	Sicherheit- 1.7 control/RDS

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.19	Sicherheit- 1.9 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.2	Sicherheit- control/RDS .2
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.20	Sicherheit- 2.0 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.21	Sicherheit- 2.1 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS2.2	Sicherheit- 2.2 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.23	Sicherheit- 2.3 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.24	Sicherheit- 2.4 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.25	Sicherheit- 2.5 control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS3.	Sicherheit- control/RDS 3.
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.4	Sicherheit- 4. control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.5	Sicherheit- 5. control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.6	Sicherheit- 6. control/RDS

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.7	Sicherheit- 7. control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.8	Sicherheit- 8. control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/RDS.9	Sicherheit- 9. control/RDS
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift1.	Sicherheit- control/Redshift 1.
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift.2	Sicherheit- control/Redshift .2
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift3.	Sicherheit- control/Redshift 3.
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift.4	Sicherheit- 4. control/Redshift
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift.6	Sicherheit- 6. control/Redshift
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift.7	Sicherheit- 7. control/Redshift
aws-fundamentale-security-best- /1.0. practices /v 0/Redshift.8	Sicherheit- 8. control/Redshift
aws-fundamentale-security-best- /1.0. practices /v 0/S31.	Sicherheit- control/S3 1.
aws-fundamentale-security-best- /1.0. practices /v 0/S3.12	Sicherheit- 1.2 control/S3

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/S3.13	Sicherheit- 1.3 control/S3
aws-fundamentale-security-best- /1.0. practices /v 0/S3.2	Sicherheit- control/S3 .2
aws-fundamentale-security-best- /1.0. practices /v 0/S33.	Sicherheit- control/S3 3.
aws-fundamentale-security-best- /1.0. practices /v 0/S3.5	Sicherheit- 5. control/S3
aws-fundamentale-security-best- /1.0. practices /v 0/S3.6	Sicherheit- 6. control/S3
aws-fundamentale-security-best- /1.0. practices /v 0/S3.8	Sicherheit- 8. control/S3
aws-fundamentale-security-best- /1.0. practices /v 0/S3.9	Sicherheit- 9. control/S3
aws-fundamentale-security-best- /1.0. practices /v 0/SageMaker1.	Sicherheit- control/SageMaker 1.
aws-fundamentale-security-best- /1.0. practices /v 0/SageMaker.2	Sicherheit- control/SageMaker .2
aws-fundamentale-security-best- /1.0. practices /v 0/SageMaker3.	Sicherheit- control/SageMaker 3.
aws-fundamentale-security-best- /1.0. practices /v 0/SecretsManager1.	Sicherheit- control/SecretsManager 1.
aws-fundamentale-security-best- /1.0. practices /v 0/SecretsManager.2	Sicherheit- control/SecretsManager .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/SecretsManager3.	Sicherheit- control/SecretsManager 3.
aws-fundamentale-security-best- /1.0. practices /v 0/SecretsManager.4	Sicherheit- 4. control/SecretsManager
aws-fundamentale-security-best- /1.0. practices /v 0/SQS1.	Sicherheit- control/SQS 1.
aws-fundamentale-security-best- /1.0. practices /v 0/SSM1.	Sicherheit- control/SSM 1.
aws-fundamentale-security-best- /1.0. practices /v 0/SSM.2	Sicherheit- control/SSM .2
aws-fundamentale-security-best- /1.0. practices /v 0/SSM3.	Sicherheit- control/SSM 3.
aws-fundamentale-security-best- /1.0. practices /v 0/SSM.4	Sicherheit- 4. control/SSM
aws-fundamentale-security-best- /1.0. practices /v 0/WAF1.	Sicherheit- control/WAF 1.
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.2	Sicherheit- control/WAF .2
aws-fundamentale-security-best- /1.0. practices /v 0/WAF3.	Sicherheit- control/WAF 3.
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.4	Sicherheit- 4. control/WAF
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.6	Sicherheit- 6. control/WAF

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.7	Sicherheit- 7. control/WAF
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.8	Sicherheit- 8. control/WAF
aws-fundamentale-security-best- /1.0. practices /v 0/WAF.10	Sicherheit- 1.0 control/WAF
pci- /3.2. dss/v 1/PCI. AutoScaling.1	Sicherheit- control/AutoScaling 1.
pci- dss/v /3.2. 1/PCI. CloudTrail.1	Sicherheit- control/CloudTrail 2.
pci- dss/v /3.2. 1/PCI. CloudTrail.2	Sicherheit- control/CloudTrail 3.
pci- dss/v /3.2. 1/PCI. CloudTrail.3	Sicherheit- control/CloudTrail 4.
pci- /3.2. dss/v 1/PCI. CloudTrail.4	Sicherheit- control/CloudTrail 5.
pci- /3.2. dss/v 1/PCI. CodeBuild.1	Sicherheit- control/CodeBuild 1.
pci- dss/v /3.2. 1/PCI. CodeBuild.2	Sicherheit- control/CodeBuild 2.
pci- dss/v /3.2. 1/PCI. Config.1	Sicherheit- control/Config 1.
pci- dss/v /3.2. 1/PCI. CW.1	Sicherheit- control/CloudWatch 1.
pci- dss/v /3.2. 1/PCI. DMS.1	Sicherheit- control/DMS 1.
pci- dss/v /3.2. 1/PCI. EC2.1	Sicherheit- control/EC2 1.
pci- dss/v /3.2. 1/PCI. EC2.2	Sicherheit- control/EC2 2.
pci- dss/v /3.2. 1/PCI. EC2.4	Sicherheit- control/EC2 1.2
pci- /3.2. dss/v 1/PCI. EC2.5	Sicherheit- control/EC2 1.3
pci- /3.2. dss/v 1/PCI. EC2.6	Sicherheit- control/EC2 6.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
pci- /3.2. dss/v 1/PCI. ELBv2.1	Sicherheit- control/ELB 1.
pci- dss/v /3.2. 1/PCI. ES.1	Sicherheit- control/ES 2.
pci- dss/v /3.2. 1/PCI. ES.2	Sicherheit- control/ES 1.
pci- dss/v /3.2. 1/PCI. GuardDuty.1	Sicherheit- control/GuardDuty 1.
pci- dss/v /3.2. 1/PCI. IAM.1	Sicherheit- control/IAM 4.
pci- /3.2. dss/v 1/PCI. IAM.2	Sicherheit- control/IAM 2.
pci- dss/v /3.2. 1/PCI. IAM.3	Sicherheit- control/IAM 1.
pci- dss/v /3.2. 1/PCI. IAM.4	Sicherheit- control/IAM 6.
pci- /3.2. dss/v 1/PCI. IAM.5	Sicherheit- control/IAM 9.
pci- /3.2. dss/v 1/PCI. IAM.6	Sicherheit- control/IAM 1.9
pci- /3.2. dss/v 1/PCI. IAM.7	Sicherheit- control/IAM 8.
pci- /3.2. dss/v 1/PCI. IAM.8	Sicherheit- control/IAM 1.0
pci- /3.2. dss/v 1/PCI. KMS.1	Sicherheit- control/KMS 4.
pci- /3.2. dss/v 1/PCI. Lambda.1	Sicherheit- control/Lambda 1.
pci- dss/v /3.2. 1/PCI. Lambda.2	Sicherheit- control/Lambda 3.
pci- dss/v /3.2. 1/PCI. Opensearch.1	Sicherheit- control/Opensearch 2.
pci- dss/v /3.2. 1/PCI. Opensearch.2	Sicherheit- control/Opensearch 1.
pci- dss/v /3.2. 1/PCI. RDS.1	Sicherheit- control/RDS 1.
pci- dss/v /3.2. 1/PCI. RDS.2	Sicherheit- control/RDS 2.
pci- dss/v /3.2. 1/PCI. Redshift.1	Sicherheit- control/Redshift 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
pci- dss/v /3.2. 1/PCI. S3.1	Sicherheit- control/S3 3.
pci- dss/v /3.2. 1/PCI. S3.2	Sicherheit- control/S3 2.
pci- dss/v /3.2. 1/PCI. S3.3	Sicherheit- control/S3 7.
pci- /3.2. dss/v 1/PCI. S3.5	Sicherheit- control/S3 5.
pci- /3.2. dss/v 1/PCI. S3.6	Sicherheit- control/S3 1.
pci- dss/v /3.2. 1/PCI. SageMaker.1	Sicherheit- control/SageMaker 1.
pci- dss/v /3.2. 1/PCI. SSM.1	Sicherheit- control/SSM 2.
pci- dss/v /3.2. 1/PCI. SSM.2	Sicherheit- control/SSM 3.
pci- dss/v /3.2. 1/PCI. SSM.3	Sicherheit- control/SSM 1.
servicemanaged-aws-control- /1.0. tower/v 0/ ACM1.	Sicherheit- control/ACM 1.
servicemanaged-aws-control- /1.0. tower/v 0/ APIGateway1.	Sicherheit- control/APIGateway 1.
servicemanaged-aws-control- /1.0. tower/v 0/ APIGateway2.	Sicherheit- control/APIGateway .2
servicemanaged-aws-control- /1.0. tower/v 0/ APIGateway3.	Sicherheit- control/APIGateway 3.
servicemanaged-aws-control- /1.0. tower/v 0/ APIGateway.4	Sicherheit- 4. control/APIGateway
servicemanaged-aws-control- /1.0. tower/v 0/ APIGateway.5	Sicherheit- 5. control/APIGateway
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling1.	Sicherheit- control/AutoScaling 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling2.	Sicherheit- control/AutoScaling .2
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling3.	Sicherheit- control/AutoScaling 3.
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling.4	Sicherheit- 4. control/AutoScaling
servicemanaged-aws-control- /1.0. tower/v 0/ Autoscaling.5	Sicherheit- 5. control/Autoscaling
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling.6	Sicherheit- 6. control/AutoScaling
servicemanaged-aws-control- /1.0. tower/v 0/ AutoScaling.9	Sicherheit- 9. control/AutoScaling
servicemanaged-aws-control- /1.0. tower/v 0/ CloudTrail1.	Sicherheit- control/CloudTrail 1.
servicemanaged-aws-control- /1.0. tower/v 0/ CloudTrail2.	Sicherheit- control/CloudTrail .2
servicemanaged-aws-control- /1.0. tower/v 0/ CloudTrail.4	Sicherheit- 4. control/CloudTrail
servicemanaged-aws-control- /1.0. tower/v 0/ CloudTrail.5	Sicherheit- 5. control/CloudTrail
servicemanaged-aws-control- /1.0. tower/v 0/ CodeBuild1.	Sicherheit- control/CodeBuild 1.
servicemanaged-aws-control- /1.0. tower/v 0/ CodeBuild2.	Sicherheit- control/CodeBuild .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ CodeBuild.4	Sicherheit- 4. control/CodeBuild
servicemanaged-aws-control- /1.0. tower/v 0/ DMS1.	Sicherheit- control/DMS 1.
servicemanaged-aws-control- /1.0. tower/v 0/ DynamoDB1.	Sicherheit- control/DynamoDB 1.
servicemanaged-aws-control- /1.0. tower/v 0/ DynamoDB2.	Sicherheit- control/DynamoDB .2
servicemanaged-aws-control- /1.0. tower/v 0/ EC21.	Sicherheit- control/EC2 1.
servicemanaged-aws-control- /1.0. tower/v 0/ EC22.	Sicherheit- control/EC2 .2
servicemanaged-aws-control- /1.0. tower/v 0/ EC23.	Sicherheit- control/EC2 3.
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.4	Sicherheit- 4. control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.6	Sicherheit- 6. control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.7	Sicherheit- 7. control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.8	Sicherheit- 8. control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.9	Sicherheit- 9. control/EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.10	Sicherheit- 1.0 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.15	Sicherheit- 1.5 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.16	Sicherheit- 1.6 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.17	Sicherheit- 1.7 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.18	Sicherheit- 1.8 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.19	Sicherheit- 1.9 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC2.20	Sicherheit- 2.0 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC22.1	Sicherheit- 2.1 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ EC22.2	Sicherheit- 2.2 control/EC2
servicemanaged-aws-control- /1.0. tower/v 0/ ECR1.	Sicherheit- control/ECR 1.
servicemanaged-aws-control- /1.0. tower/v 0/ ECR2.	Sicherheit- control/ECR .2
servicemanaged-aws-control- /1.0. tower/v 0/ ECR3.	Sicherheit- control/ECR 3.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ ECS2.	Sicherheit- control/ECS .2
servicemanaged-aws-control- /1.0. tower/v 0/ ECS3.	Sicherheit- control/ECS 3.
servicemanaged-aws-control- /1.0. tower/v 0/ ECS.4	Sicherheit- 4. control/ECS
servicemanaged-aws-control- /1.0. tower/v 0/ ECS.5	Sicherheit- 5. control/ECS
servicemanaged-aws-control- /1.0. tower/v 0/ ECS.8	Sicherheit- 8. control/ECS
servicemanaged-aws-control- /1.0. tower/v 0/ ECS.10	Sicherheit- 1.0 control/ECS
servicemanaged-aws-control- /1.0. tower/v 0/ ECS.12	Sicherheit- 1.2 control/ECS
servicemanaged-aws-control- /1.0. tower/v 0/ EFS1.	Sicherheit- control/EFS 1.
servicemanaged-aws-control- /1.0. tower/v 0/ EFS2.	Sicherheit- control/EFS .2
servicemanaged-aws-control- /1.0. tower/v 0/ EFS3.	Sicherheit- control/EFS 3.
servicemanaged-aws-control- /1.0. tower/v 0/ EFS.4	Sicherheit- 4. control/EFS
servicemanaged-aws-control- /1.0. tower/v 0/ EKS2.	Sicherheit- control/EKS .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ ELB2.	Sicherheit- control/ELB .2
servicemanaged-aws-control- /1.0. tower/v 0/ ELB3.	Sicherheit- control/ELB 3.
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.4	Sicherheit- 4. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.5	Sicherheit- 5. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.6	Sicherheit- 6. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.7	Sicherheit- 7. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.8	Sicherheit- 8. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.9	Sicherheit- 9. control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.10	Sicherheit- 1.0 control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.12	Sicherheit- 1.2 control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB1.3	Sicherheit- 1.3 control/ELB
servicemanaged-aws-control- /1.0. tower/v 0/ ELB.14	Sicherheit- 1.4 control/ELB

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ ELBv21.	Sicherheit- control/ELBv2 1.
servicemanaged-aws-control- /1.0. tower/v 0/ EMR1.	Sicherheit- control/EMR 1.
servicemanaged-aws-control- /1.0. tower/v 0/ ES1.	Sicherheit- control/ES 1.
servicemanaged-aws-control- /1.0. tower/v 0/ ES2.	Sicherheit- control/ES .2
servicemanaged-aws-control- /1.0. tower/v 0/ ES3.	Sicherheit- control/ES 3.
servicemanaged-aws-control- /1.0. tower/v 0/ ES.4	Sicherheit- 4. control/ES
servicemanaged-aws-control- /1.0. tower/v 0/ ES.5	Sicherheit- 5. control/ES
servicemanaged-aws-control- /1.0. tower/v 0/ ES.6	Sicherheit- 6. control/ES
servicemanaged-aws-control- /1.0. tower/v 0/ ES.7	Sicherheit- 7. control/ES
servicemanaged-aws-control- /1.0. tower/v 0/ ES.8	Sicherheit- 8. control/ES
servicemanaged-aws-control- /1.0. tower/v 0/ ElasticBeanstalk1.	Sicherheit- control/ElasticBeanstalk 1.
servicemanaged-aws-control- /1.0. tower/v 0/ ElasticBeanstalk2.	Sicherheit- control/ElasticBeanstalk .2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ GuardDuty1.	Sicherheit- control/GuardDuty 1.
servicemanaged-aws-control- /1.0. tower/v 0/ IAM1.	Sicherheit- control/IAM 1.
servicemanaged-aws-control- /1.0. tower/v 0/ IAM2.	Sicherheit- control/IAM .2
servicemanaged-aws-control- /1.0. tower/v 0/ IAM3.	Sicherheit- control/IAM 3.
servicemanaged-aws-control- /1.0. tower/v 0/ IAM.4	Sicherheit- 4. control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ IAM.5	Sicherheit- 5. control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ IAM.6	Sicherheit- 6. control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ IAM.7	Sicherheit- 7. control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ IAM.8	Sicherheit- 8. control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ IAM2.1	Sicherheit- 2.1 control/IAM
servicemanaged-aws-control- /1.0. tower/v 0/ Kinesis1.	Sicherheit- control/Kinesis 1.
servicemanaged-aws-control- /1.0. tower/v 0/ KMS1.	Sicherheit- control/KMS 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ KMS2.	Sicherheit- control/KMS .2
servicemanaged-aws-control- /1.0. tower/v 0/ KMS3.	Sicherheit- control/KMS 3.
servicemanaged-aws-control- /1.0. tower/v 0/ Lambda1.	Sicherheit- control/Lambda 1.
servicemanaged-aws-control- /1.0. tower/v 0/ Lambda2.	Sicherheit- control/Lambda .2
servicemanaged-aws-control- /1.0. tower/v 0/ Lambda.5	Sicherheit- 5. control/Lambda
servicemanaged-aws-control- /1.0. tower/v 0/ NetworkFirewall3.	Sicherheit- control/NetworkFirewall 3.
servicemanaged-aws-control- /1.0. tower/v 0/ NetworkFirewall.4	Sicherheit- 4. control/NetworkFirewall
servicemanaged-aws-control- /1.0. tower/v 0/ NetworkFirewall.5	Sicherheit- 5. control/NetworkFirewall
servicemanaged-aws-control- /1.0. tower/v 0/ NetworkFirewall.6	Sicherheit- 6. control/NetworkFirewall
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch1.	Sicherheit- control/Opensearch 1.
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch2.	Sicherheit- control/Opensearch .2
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch3.	Sicherheit- control/Opensearch 3.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch.4	Sicherheit- 4. control/Opensearch
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch.5	Sicherheit- 5. control/Opensearch
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch.6	Sicherheit- 6. control/Opensearch
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch.7	Sicherheit- 7. control/Opensearch
servicemanaged-aws-control- /1.0. tower/v 0/ Opensearch.8	Sicherheit- 8. control/Opensearch
servicemanaged-aws-control- /1.0. tower/v 0/ RDS1.	Sicherheit- control/RDS 1.
servicemanaged-aws-control- /1.0. tower/v 0/ RDS2.	Sicherheit- control/RDS .2
servicemanaged-aws-control- /1.0. tower/v 0/ RDS3.	Sicherheit- control/RDS 3.
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.4	Sicherheit- 4. control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.5	Sicherheit- 5. control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.6	Sicherheit- 6. control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.8	Sicherheit- 8. control/RDS

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.9	Sicherheit- 9. control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.10	Sicherheit- 1.0 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.11	Sicherheit- 1.1 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS1.3	Sicherheit- 1.3 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.17	Sicherheit- 1.7 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.19	Sicherheit- 1.9 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS.20	Sicherheit- 2.0 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS2.1	Sicherheit- 2.1 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS2.2	Sicherheit- 2.2 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS2.3	Sicherheit- 2.3 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ RDS2,5	Sicherheit- 2.5 control/RDS
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift1.	Sicherheit- control/Redshift 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift2.	Sicherheit- control/Redshift .2
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift.4	Sicherheit- 4. control/Redshift
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift.6	Sicherheit- 6. control/Redshift
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift.7	Sicherheit- 7. control/Redshift
servicemanaged-aws-control- /1.0. tower/v 0/ Redshift.8	Sicherheit- 8. control/Redshift
servicemanaged-aws-control- /1.0. tower/v 0/ S31.	Sicherheit- control/S3 1.
servicemanaged-aws-control- /1.0. tower/v 0/ S32.	Sicherheit- control/S3 .2
servicemanaged-aws-control- /1.0. tower/v 0/ S33.	Sicherheit- control/S3 3.
servicemanaged-aws-control- /1.0. tower/v 0/ S3.5	Sicherheit- 5. control/S3
servicemanaged-aws-control- /1.0. tower/v 0/ S3.6	Sicherheit- 6. control/S3
servicemanaged-aws-control- /1.0. tower/v 0/ S3.8	Sicherheit- 8. control/S3
servicemanaged-aws-control- /1.0. tower/v 0/ S3.9	Sicherheit- 9. control/S3

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ S3.12	Sicherheit- 1.2 control/S3
servicemanaged-aws-control- /1.0. tower/v 0/ S31.3	Sicherheit- 1.3 control/S3
servicemanaged-aws-control- /1.0. tower/v 0/ SageMaker1.	Sicherheit- control/SageMaker 1.
servicemanaged-aws-control- /1.0. tower/v 0/ SecretsManager1.	Sicherheit- control/SecretsManager 1.
servicemanaged-aws-control- /1.0. tower/v 0/ SecretsManager2.	Sicherheit- control/SecretsManager .2
servicemanaged-aws-control- /1.0. tower/v 0/ SecretsManager3.	Sicherheit- control/SecretsManager 3.
servicemanaged-aws-control- /1.0. tower/v 0/ SecretsManager.4	Sicherheit- 4. control/SecretsManager
servicemanaged-aws-control- /1.0. tower/v 0/ SQS1.	Sicherheit- control/SQS 1.
servicemanaged-aws-control- /1.0. tower/v 0/ SSM1.	Sicherheit- control/SSM 1.
servicemanaged-aws-control- /1.0. tower/v 0/ SSM2.	Sicherheit- control/SSM .2
servicemanaged-aws-control- /1.0. tower/v 0/ SSM3.	Sicherheit- control/SSM 3.
servicemanaged-aws-control- /1.0. tower/v 0/ SSM.4	Sicherheit- 4. control/SSM

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
servicemanaged-aws-control- /1.0. tower/v 0/ WAF2.	Sicherheit- control/WAF .2
servicemanaged-aws-control- /1.0. tower/v 0/ WAF3.	Sicherheit- control/WAF 3.
servicemanaged-aws-control- /1.0. tower/v 0/ WAF.4	Sicherheit- 4. control/WAF

Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt

Die Ansicht konsolidierter Kontrollen und die konsolidierten Kontrollergebnisse vereinheitlichen Kontroll-IDs und Titel für alle Standards. Die Begriffe Security Control ID und Security Control Title beziehen sich auf diese standardunabhängigen Werte.

Die Security Hub CSPM-Konsole zeigt standardunabhängige Sicherheitskontroll-IDs und Sicherheitskontrolltitel an, unabhängig davon, ob die konsolidierten Kontrollergebnisse für Ihr Konto aktiviert oder deaktiviert sind. Die CSPM-Ergebnisse von Security Hub enthalten jedoch standardspezifische Kontrolltitel für PCI DSS und CIS v1.2.0, falls konsolidierte Kontrollergebnisse für Ihr Konto deaktiviert sind. Darüber hinaus enthalten die Ergebnisse des Security Hub CSPM die standardspezifische Kontroll-ID und die Sicherheitskontroll-ID. Beispiele dafür, wie sich die Konsolidierung auf die Kontrollergebnisse auswirkt, finden Sie unter. Stichproben von Kontrollbefunden

Bei Kontrollen, die Teil des AWS Control Tower Service-Managed-Standards sind, `CT.` wird das Präfix aus der Kontroll-ID und dem Titel in den Ergebnissen entfernt, wenn konsolidierte Kontrollergebnisse aktiviert sind.

Um eine Sicherheitskontrolle in Security Hub CSPM zu deaktivieren, müssen Sie alle Standardsteuerungen deaktivieren, die der Sicherheitskontrolle entsprechen. Die folgende Tabelle zeigt die Zuordnung von IDs und Titeln für Sicherheitskontrollen zu standardspezifischen Kontroll-IDs und Titeln. IDs und Titel für Kontrollen, die zum FSBP-Standard (AWS Foundation Security Best Practices) gehören, sind bereits standardunabhängig. Eine Zuordnung der Steuerelemente zu den Anforderungen von Center for Internet Security (CIS) v3.0.0 finden Sie unter. Zuordnung der

Kontrollen zu den CIS-Anforderungen in jeder Version Um Ihre eigenen Skripts für diese Tabelle auszuführen, können Sie sie als CSV-Datei herunterladen.

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.1 Vermeiden Sie die Verwendung des Root-Benutzers	[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
CIS v1.2.0	1.10 Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern	[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
CIS v1.2.0	1.11 Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
CIS v1.2.0	1.12 Stellen Sie sicher, dass kein Root-Benutzerzugriffsschlüssel vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.2.0	1.13 Stellen Sie sicher, dass MFA für den Root-Benutzer aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.2.0	1.14 Stellen Sie sicher, dass Hardware-MFA für den Root-Benutzer aktiviert ist	[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.2.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien nur Gruppen oder Rollen zugeordnet sind	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
CIS v1.2.0	1.2 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen	[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.20 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde Support	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
CIS v1.2.0	1.22 Stellen Sie sicher, dass keine IAM-Richtlinien erstellt werden, die volle „*: *“ -Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
CIS v1.2.0	1.3 Stellen Sie sicher, dass Anmeldeinformationen, die 90 Tage oder länger nicht verwendet wurden, deaktiviert sind	[IAM.8] Unbenutzte IAM-Benut zeranmeldedaten sollten entfernt werden
CIS v1.2.0	1.4 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.2.0	1.5 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
CIS v1.2.0	1.6 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
CIS v1.2.0	1.7 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert	[IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
CIS v1.2.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.2.0	2.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.2.0	2.2 Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.2.0	2.3 Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
CIS v1.2.0	2.4 Stellen Sie sicher, dass die CloudTrail Pfade in CloudWatch Logs integriert sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
CIS v1.2.0	2.5 Stellen Sie sicher, dass AWS Config es aktiviert ist	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden
CIS v1.2.0	2.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	2.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezustand mithilfe von KMS-CMKs verschlüsselt werden	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.2.0	2.8 Stellen Sie sicher, dass die Rotation für vom Kunden erstellte CMKs aktiviert ist	[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein
CIS v1.2.0	2.9 Stellen Sie sicher, dass die VPC-Flussprotokollierung in allen VPCs aktiviert ist	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
CIS v1.2.0	3.1 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
CIS v1.2.0	3.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
CIS v1.2.0	3.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
CIS v1.2.0	3.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
CIS v1.2.0	3.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.2.0	3.2 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung in der Management Console ohne MFA vorhanden sind	[CloudWatch.3] Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind
CIS v1.2.0	3.3 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Verwendung des Root-Benutzers vorhanden sind	[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
CIS v1.2.0	3.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
CIS v1.2.0	3.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind
CIS v1.2.0	3.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS-Managementkonsole Authentifizierungsfehler vorhanden sind	[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.2.0	3.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind
CIS v1.2.0	3.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration
CIS v1.2.0	4.1 Stellen Sie sicher, dass keine Sicherheitsgruppen Zugriffe ab Version 0.0.0 zulassen. 0/0 zu Port 22	[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22
CIS v1.2.0	4.2 Stellen Sie sicher, dass keine Sicherheitsgruppen Zugriffe ab Version 0.0.0 zulassen. 0/0 zu Port 3389	[EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
CIS v1.2.0	4.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	1.10 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen	[IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
CIS v1.4.0	1.14 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.4.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien, die volle „*: *“ -Administratorrechte zulassen, nicht beigefügt sind	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
CIS v1.4.0	1.17 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde Support	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
CIS v1.4.0	1.4 Stellen Sie sicher, dass kein Zugriffsschlüssel für das Root-Benutzerkonto vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.4.0	1.5 Stellen Sie sicher, dass MFA für das Root-Benutzerkonto aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.4.0	1.6 Stellen Sie sicher, dass Hardware-MFA für das Root-Benutzerkonto aktiviert ist	[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.4.0	1.7 Eliminieren Sie die Verwendung des Root-Benutzers für administrative und tägliche Aufgaben	[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.4.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederver wendung von	[IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederver wendung von Passwörtern
CIS v1.4.0	2.1.2 Stellen Sie sicher, dass die S3-Bucket-Richtlinie so eingestellt ist, dass HTTP-Anfragen abgelehnt werden	[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein
CIS v1.4.0	2.1.5.1 Die Einstellung S3 Block Public Access sollte aktiviert sein	[S3.1] Für S3-Allzweck-Bucket s sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
CIS v1.4.0	2.1.5.2 Die Einstellung S3 Block Public Access sollte auf Bucket-Eb ene aktiviert sein	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
CIS v1.4.0	2.2.1 Stellen Sie sicher, dass die EBS-Volume-Verschlüsselung aktiviert ist	[EC2.7] Die EBS-Standardversch lüsselung sollte aktiviert sein
CIS v1.4.0	2.3.1 Stellen Sie sicher, dass die Verschlüsselung für RDS-Instances aktiviert ist	[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	3.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.4.0	3.2 Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.4.0	3.4 Stellen Sie sicher, dass die CloudTrail Pfade in Logs integriert CloudWatch sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
CIS v1.4.0	3.5 Stellen Sie sicher, dass AWS Config es in allen Regionen aktiviert ist	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden
CIS v1.4.0	3.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
CIS v1.4.0	3.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezustand mithilfe von KMS-CMKs verschlüsselt werden	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.4.0	3.8 Stellen Sie sicher, dass die Rotation für vom Kunden erstellte CMKs aktiviert ist	[KMS.4] AWS KMS Die Schlüsselrotation sollte aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	3.9 Stellen Sie sicher, dass die VPC-Flussprotokollierung in allen VPCs aktiviert ist	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
CIS v1.4.0	4.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
CIS v1.4.0	4.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind
CIS v1.4.0	4.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS-Managementkonsole Authentifizierungsfehler vorhanden sind	[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS-Managementkonsole Fehler bei der Authentifizierung
CIS v1.4.0	4.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.4.0	4.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinien vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	4.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind für AWS Config Änderungen an der Konfiguration
CIS v1.4.0	4.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
CIS v1.4.0	4.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
CIS v1.4.0	4.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
CIS v1.4.0	4.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
CIS v1.4.0	4.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.4.0	5.1 Stellen Sie sicher, dass keine Netzwerk-ACLs den Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers	[EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	5.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
PCI DSS v3.2.1	PCI.AutoScaling.1 Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Zustandsprüfungen verwenden	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail Protokolle sollten im Ruhezustand mithilfe von CMKs verschlüsselt werden AWS KMS	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail sollte aktiviert sein	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub oder Bitbucket-Quell-Repository-URLs sollten OAuth verwenden	[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.Config.1 AWS Config sollte aktiviert sein	[Config.1] AWS Config sollte aktiviert sein und die dienstbezogene Rolle für die Ressourcenaufzeichnung verwenden
PCI DSS v3.2.1	PCI.CW.1 Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein	[CloudWatch.1] Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein
PCI DSS v3.2.1	PCI.DMS.1 Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein	[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
PCI DSS v3.2.1	PCI.EC2.1 EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	[EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind
PCI DSS v3.2.1	PCI.EC2.2 Die VPC-Standardsicher heitsgruppe sollte eingehenden und ausgehenden Datenverkehr verbieten	[EC2.2] VPC-Standardsicher heitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
PCI DSS v3.2.1	PCI.EC2.4 Ungenutzte EC2-EIPs sollten entfernt werden	[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
PCI DSS v3.2.1	PCI.EC2.5 Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22	[EC2.13] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 oder: :/0 zu Port 22
PCI DSS v3.2.1	PCI.EC2.6 Die VPC-Flussprotokoll ierung sollte in allen VPCs aktiviert sein	[EC2.6] Die VPC-Flow-Protokoll ierung sollte in allen VPCs aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.ELBv2.1 Der Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden.	[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch-Domains sollten sich in einer VPC befinden	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
PCI DSS v3.2.1	PCI.ES.2 Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	[ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty sollte aktiviert sein	[GuardDuty.1] GuardDuty sollte aktiviert sein
PCI DSS v3.2.1	PCI.IAM.1 Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
PCI DSS v3.2.1	PCI.IAM.2 IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
PCI DSS v3.2.1	PCI.IAM.3 IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
PCI DSS v3.2.1	PCI.IAM.4 Hardware-MFA sollte für den Root-Benutzer aktiviert sein	[IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.5 Virtual MFA sollte für den Root-Benutzer aktiviert sein	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.6 MFA sollte für alle IAM-Benutzer aktiviert sein	[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.IAM.7 IAM-Benutzeranmeld edaten sollten deaktiviert werden, wenn sie nicht innerhalb einer vordefinierten Anzahl von Tagen verwendet werden	[IAM.8] Unbenutzte IAM-Benut zeranmeldedaten sollten entfernt werden
PCI DSS v3.2.1	PCI.IAM.8 Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben	[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguri ert sein
PCI DSS v3.2.1	PCI.KMS.1 Die CMK-Rotation (Customer Master Key) sollte aktiviert sein	[KMS.4] AWS KMS Die Schlüssel rotation sollte aktiviert sein
PCI DSS v3.2.1	PCI.Lambda.1 Lambda-Funktionen sollten den öffentlichen Zugriff verbieten	[Lambda.1] Lambda-Funktionsri chtlinien sollten den öffentlichen Zugriff verbieten
PCI DSS v3.2.1	PCI.Lambda.2 Lambda-Funktionen sollten sich in einer VPC befinden	[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch Domains sollten sich in einer VPC befinden	[Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
PCI DSS v3.2.1	PCI.Opensearch.2 EBS-Snapshots sollten nicht öffentlich wiederher stellbar sein	Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	PCI.RDS.1 RDS-Snapshot sollte privat sein	[RDS.1] Der RDS-Snapshot sollte privat sein
PCI DSS v3.2.1	PCI.RDS.2 RDS-DB-Instances sollten den öffentlichen Zugriff verbieten	[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
PCI DSS v3.2.1	PCI.S3.1 S3-Buckets sollten öffentlichen Schreibzugriff verbieten	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
PCI DSS v3.2.1	PCI.S3.2 S3-Buckets sollten öffentlichen Lesezugriff verbieten	[S3.2] S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren
PCI DSS v3.2.1	PCI.S3.3 Bei S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
PCI DSS v3.2.1	PCI.S3.5 S3-Buckets sollten Anfragen zur Verwendung von Secure Socket Layer erfordern	[S3.5] Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von TLS erforderlich sein
PCI DSS v3.2.1	PCI.S3.6 Die Einstellung S3 Block Public Access sollte aktiviert sein	[S3.1] Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
PCI DSS v3.2.1	PCI.SageMaker.1 SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben	[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
PCI DSS v3.2.1	PCI.SSM.1 Von Systems Manager verwaltete EC2-Instances sollten nach einer Patch-Installation den Patch-Konformitätsstatus COMPLIANT haben	[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.SSM.2 Von Systems Manager verwaltete EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben	[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
PCI DSS v3.2.1	PCI.SSM.3 EC2-Instances sollten verwaltet werden von AWS Systems Manager	[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

Aktualisierung der Workflows für die Konsolidierung

Wenn Ihre Workflows nicht auf dem spezifischen Format der Felder in den Kontrollergebnissen basieren, sind keine Maßnahmen erforderlich.

Wenn Ihre Workflows auf dem spezifischen Format eines oder mehrerer Felder in Kontrollergebnissen basieren, wie in den obigen Tabellen angegeben, sollten Sie Ihre Workflows aktualisieren. Wenn Sie beispielsweise eine EventBridge Amazon-Regel erstellt haben, die eine Aktion für eine bestimmte Kontroll-ID ausgelöst hat, z. B. das Aufrufen einer AWS Lambda Funktion, wenn die Kontroll-ID CIS 2.7 entspricht, aktualisieren Sie die zu verwendende Regel CloudTrail.2, die dem Wert für das `Compliance.SecurityControlId` Feld für dieses Steuerelement entspricht.

Wenn Sie benutzerdefinierte Erkenntnisse erstellt haben, die Felder oder Werte verwenden, die sich geändert haben, aktualisieren Sie diese Erkenntnisse, sodass sie die neuen Felder oder Werte verwenden.

Erforderliche ASFF-Attribute der obersten Ebene

Die folgenden Attribute der obersten Ebene im AWS Security Finding Format (ASFF) sind für alle Ergebnisse in Security Hub CSPM erforderlich. Weitere Informationen zu diesen Attributen finden Sie AwsSecurityFindingin der AWS Security Hub Hub-API-Referenz.

AwsAccountId

Die AWS-Konto ID, für die das Ergebnis gilt.

Beispiel

```
"AwsAccountId": "111111111111"
```

CreatedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder das Ereignis, das durch einen Befund erfasst wurde, verursacht wurde.

Beispiel

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Description

Die Beschreibung eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für die Instance des Fundes enthalten.

Für Kontrollergebnisse, die Security Hub CSPM generiert, enthält dieses Feld eine Beschreibung der Kontrolle.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

Die Kennung für die lösungsspezifische Komponente (eine separate Logikeinheit), die einen Fund generiert hat.

Bei Kontrollergebnissen, die Security Hub CSPM generiert, verweist dieses Feld nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"GeneratorId": "security-control/Config.1"
```

Id

Die produktspezifische Kennung für einen Fund. Für Kontrollergebnisse, die Security Hub CSPM generiert, enthält dieses Feld den Amazon-Ressourcennamen (ARN) des Ergebnisses.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Der von Security Hub CSPM generierte Amazon-Ressourcenname (ARN), der ein Finding-Produkt eines Drittanbieters eindeutig identifiziert, nachdem das Produkt bei Security Hub CSPM registriert wurde.

Das Format des Felds ist `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- AWS-Services Damit sie in Security Hub CSPM integriert sind, `company-id` müssen sie "`aws`" lauten, und das `product-id` muss der Name des AWS öffentlichen Dienstes sein. Da AWS Produkte und Dienstleistungen keinem Konto zugeordnet sind, ist der `account-id` Bereich des ARN leer. AWS-Services die noch nicht in Security Hub CSPM integriert sind, gelten als Produkte von Drittanbietern.
- Für öffentliche Produkte müssen die `company-id` und die `product-id` die ID-Werte sein, die zum Zeitpunkt der Registrierung angegeben wurden.
- Für private Produkte muss die `company-id` die Konto-ID sein. Die `product-id` muss das reservierte Wort "default" (Standard) oder die ID sein, die zum Zeitpunkt der Registrierung angegeben wurde.

Beispiel

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Ressourcen

Das `Resources` Array von Objekten stellt eine Reihe von Ressourcendatentypen bereit, die die AWS Ressourcen beschreiben, auf die sich das Ergebnis bezieht. Einzelheiten zu den Feldern, die ein `Resources` Objekt enthalten kann, einschließlich der Felder, die erforderlich sind, finden Sie Resourcein der AWS Security Hub Hub-API-Referenz. Beispiele für bestimmte `Resources` Objekte finden Sie AWS-Services unterRessourcen ASFF-Objekt.

Beispiel

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
```

```
                    }
                },
                {
                    "Count": 59,
                    "Type": "EMAIL_ADDRESS",
                    "Occurrences": {
                        "Pages": [
                            {
                                "PageNumber": 1,
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                            {
                                "Start": 1,
                                "End": 13
                            }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
```

```
                            ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
```

```
    "InstanceMetadataTags": "disabled"
   }
  },
   "NetworkInterfaces": [
   {
    "NetworkInterfaceId": "eni-e5aa89a3"
   }
   ],
   "SubnetId": "PublicSubnet",
   "Type": "i3.xlarge",
   "VirtualizationType": "hvm",
   "VpcId": "TestVPCIpv6"
  }

]
```

SchemaVersion

Die Schemaversion, für die ein Fund formatiert ist. Der Wert dieses Feldes muss eine der offiziell veröffentlichten Versionen sein, die von AWS identifiziert wurden. In der aktuellen Version ist die Schemaversion des AWS Security Finding Formats`2018-10-08`.

Beispiel

```
"SchemaVersion": "2018-10-08"
```

Schweregrad

Definiert die Wichtigkeit eines Ergebnisses. Einzelheiten zu diesem Objekt finden Sie `Severity`in der AWS Security Hub API-Referenz.

`Severity`ist sowohl ein Objekt der obersten Ebene in einem Finding als auch ein unter dem Objekt verschachteltes Objekt. `FindingProviderFields`

Der Wert des `Severity` Objekts der obersten Ebene für einen Befund sollte nur mithilfe der API aktualisiert werden. `BatchUpdateFindings`

Um Informationen zum Schweregrad bereitzustellen, sollten Suchanbieter `FindingProviderFields` bei einer `BatchImportFindings`API-Anfrage das `Severity` Objekt unter aktualisieren.

Wenn eine `BatchImportFindings` Anfrage für ein neues Ergebnis nur liefert `Label` oder nur liefert`Normalized`, füllt Security Hub CSPM automatisch den Wert des anderen Felds aus. Die `Original` Felder `Product` und können ebenfalls ausgefüllt werden.

Wenn das `Finding.Severity` Objekt der obersten Ebene vorhanden, aber nicht vorhanden `Finding.FindingProviderFields` ist, erstellt Security Hub CSPM das `FindingProviderFields.Severity` Objekt und kopiert das gesamte `Finding.Severity` `object` Objekt hinein. Dadurch wird sichergestellt, dass die ursprünglichen, vom Anbieter bereitgestellten Details in der `FindingProviderFields.Severity` Struktur beibehalten werden, auch wenn das Objekt der obersten Ebene überschrieben wird. `Severity`

Der Schweregrad des Ergebnisses berücksichtigt nicht den kritischen Charakter der beteiligten Komponenten oder der zugrunde liegenden Ressource. Der kritische Charakter ist definiert als die Wichtigkeit der Ressourcen, die mit dem Ergebnis verbunden sind. Beispielsweise hat eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, eine höhere Priorität als eine Ressource, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das `Criticality`-Feld, um Informationen zum kritischen Charakter der Ressource zu erfassen.

Wir empfehlen, bei der Übersetzung der systemeigenen Schweregrade der Ergebnisse in den Wert von im ASFF die folgenden Hinweise zu beachten. `Severity.Label`

- `INFORMATIONAL`— Diese Kategorie kann einen Befund für einen`PASSED`,`WARNING`, oder `NOT AVAILABLE` Scheck oder eine Identifizierung sensibler Daten beinhalten.
- `LOW`— Erkenntnisse, die zu future Kompromissen führen könnten. Zu dieser Kategorie können beispielsweise Sicherheitslücken, Konfigurationsschwächen und offengelegte Passwörter gehören.
- `MEDIUM`— Ergebnisse, die auf einen aktiven Kompromiss hindeuten, aber keinen Hinweis darauf, dass ein Gegner seine Ziele erreicht hat. Zu dieser Kategorie können beispielsweise Malware-Aktivitäten, Hacking-Aktivitäten und die Erkennung ungewöhnlicher Verhaltensweisen gehören.
- `HIGH`oder `CRITICAL` — Ergebnisse, die darauf hindeuten, dass ein Angreifer seine Ziele erreicht hat, wie z. B. aktiver Datenverlust oder Datenkompromittierung oder Denial-of-Service.

Beispiel

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Title

Der Titel eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für diese Instanz des Fundes enthalten.

Bei Kontrollergebnissen gibt dieses Feld den Titel der Kontrolle an. Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Title": "AWS Config should be enabled"
```

Typen

Ein oder mehrere Fundtypen im Format *namespace*/*category*/*classifier*, die einen Fund klassifizieren. Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`Types`sollte nur mithilfe der `BatchUpdateFindings`API aktualisiert werden.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Types` sollten Sie das `Types` Attribut unter verwenden `FindingProviderFields`.

In der folgenden Liste sind die Aufzählungszeichen der obersten Ebene Namespaces, die Aufzählungszeichen der zweiten Ebene sind Kategorien und die Aufzählungszeichen der dritten Ebene sind Klassifikatoren. Wir empfehlen, dass Suchanbieter definierte Namespaces verwenden, um Ergebnisse zu sortieren und zu gruppieren. Die definierten Kategorien und Klassifikatoren können ebenfalls verwendet werden, sind aber nicht erforderlich. Nur der Software- und Konfigurationsprüfungs-Namespace hat definierte Klassifizierer.

Sie können einen Teilpfad für namespace/category /classifier definieren. Beispielsweise sind die folgenden Ergebnisarten alle gültig:

- TTPs
- TTPs/Defense Ausweichen
- TTPs/Defense Evasion/CloudTrailStopped

Die Kategorien Taktiken, Techniken und Verfahren (TTPs) in der folgenden Liste entsprechen der MITRE ATT&CK MatrixTM. Der Namespace Unusual Behaviors spiegelt allgemeines ungewöhnliches Verhalten wider, wie z. B. allgemeine statistische Anomalien, und ist nicht auf ein bestimmtes TTP

abgestimmt. Sie könnten einen Fund jedoch mit beiden Fundtypen (Ungewöhnliches Verhalten und TTPs) klassifizieren.

Liste der Namespaces, Kategorien und Klassifikatoren:

- Software- und Konfigurationsprüfungen
  - Schwachstellen
    - CVE
  - AWS Bewährte Methoden im Bereich Sicherheit
    - Netzwerkerreichbarkeit
    - Laufzeitverhaltens-Analyse
  - Branchen- und regulatorische Standards
    - AWS Bewährte grundlegende Sicherheitsmethoden
    - CIS-Benchmarks zur Host-Härtung
    - Benchmark für AWS GUS-Stif
    - PCI-DSS
    - Cloud Security Alliance-Kontrollen
    - ISO 90001-Kontrollen
    - ISO 27001-Kontrollen
    - ISO 27017-Kontrollen
    - ISO 27018-Kontrollen
    - SOC 1
    - SOC 2
    - HIPAA-Kontrollen (USA)
    - NIST 800-53-Kontrollen (USA)
    - NIST CSF-Kontrollen (USA)
    - IRAP-Kontrollen (Australien)
    - K-ISMS Kontrollen (Korea)
    - MTCS-Kontrollen (Singapur)
    - FISC-Kontrollen (Japan)
    - My Number Act-Kontrollen (Japan)
    - ENS-Kontrollen (Spanien)

    - Cyber Essentials Plus-Kontrollen (Vereinigtes Königkreich)
    - G-Cloud Steuerungen (Großbritannien)
    - C5-Kontrollen (Deutschland)
    - IT-Grundschutz Controls (Deutschland)
    - DSGVO-Kontrollen (Europa)
    - TISAX-Kontrollen (Europa)
  - Patch-Management
- TTPs
  - Anfänglicher Zugriff
  - Ausführung
  - Persistenz
  - Rechteeskalation
  - Abwehrumgehung
  - Anmeldeinformationszugriff
  - Erkennung
  - Seitwärtsbewegung (Lateral Movement)
  - Sammlung
  - Command and Control
- Auswirkungen
  - Offenlegung von Daten
  - Datenexfiltration
  - Datenvernichtung
  - Denial of Service
  - Ressourcennutzung
- Ungewöhnliches Verhalten
  - Anwendung
  - Netzwerkfluss
  - IP-Adresse
  - Benutzer
  - VM

  - Behälter
  - Serverless
  - Prozess
  - Datenbank
  - Daten
- Identifizierung sensibler Daten
  - Personenbezogene Daten
  - Passwörter
  - Recht
  - Finanzanwendungen
  - Sicherheit
  - Geschäft

Beispiel

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

Gibt an, wann der Suchprovider den Ergebnisdatensatz zuletzt aktualisiert hat.

Dieser Zeitstempel gibt den Zeitpunkt an, zu dem der Suchdatensatz zuletzt oder zuletzt aktualisiert wurde. Folglich kann er vom `LastObservedAt` Zeitstempel abweichen, der angibt, wann das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde.

Wenn Sie den Funddatensatz aktualisieren, müssen Sie diesen Zeitstempel durch den aktualisierten Zeitstempel ersetzen. Bei der Erstellung eines Befunddatensatzes müssen die Zeitstempel `CreatedAt` und die `UpdatedAt` Zeitstempel identisch sein. Nach einer Aktualisierung des Suchdatensatzes muss der Wert dieses Felds aktueller sein als alle vorherigen Werte, die es enthielt.

Beachten Sie, dass dieser `BatchUpdateFindings`Vorgang `UpdatedAt` nicht aktualisiert werden kann. Sie können es nur mithilfe von `BatchImportFindings`Operation aktualisieren.

Beispiel

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Optionale ASFF-Attribute der obersten Ebene

Die folgenden Attribute der obersten Ebene im AWS Security Finding Format (ASFF) sind für Ergebnisse in Security Hub CSPM optional. Weitere Informationen zu diesen Attributen finden Sie AwsSecurityFindingin der AWS Security Hub Hub-API-Referenz.

Action

Das `Action`Objekt enthält Details zu einer Aktion, die sich auf eine Ressource auswirkt oder auf einer Ressource ausgeführt wurde.

Beispiel

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
```

```
                    "Asn": 64496
                }
            }
        }
    ],
    "Blocked": false
  }
}
```

AwsAccountName

Der AWS-Konto Name, auf den sich das Ergebnis bezieht.

Beispiel

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Der Name des Unternehmens für das Produkt, das zu dem Ergebnis geführt hat. Bei Ergebnissen, die auf Kontrollen beruhen, lautet das Unternehmen. AWS

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. `BatchImportFindings` `BatchUpdateFindings` Die Ausnahme ist, wenn Sie eine benutzerdefinierte Integration verwenden. Siehe the section called “Maßgeschneiderte Produktintegrationen”.

Wenn Sie die Security Hub CSPM-Konsole verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie dieses Attribut. Wenn Sie die Security Hub CSPM-API verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie das `aws/securityhub/CompanyName` Attribut unter. `ProductFields` Security Hub CSPM synchronisiert diese beiden Attribute nicht.

Beispiel

```
"CompanyName": "AWS"
```

Compliance

Das `Compliance`Objekt enthält in der Regel Details zu einem Kontrollergebnis, z. B. geltende Standards und den Status der Kontrollprüfung.

Beispiel

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub CSPM a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass ein Ergebnis das Verhalten oder das Problem, das identifiziert werden sollte, genau identifiziert.

`Confidence`sollte nur mit aktualisiert werden `BatchUpdateFindings`.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Confidence` sollten Sie das `Confidence` Attribut unter verwenden`FindingProviderFields`. Siehe the section called “Aktualisierung der Ergebnisse mit FindingProviderFields”.

`Confidence`wird anhand einer Verhältnisskala auf einer Basis von 0—100 bewertet. 0 bedeutet 0 Prozent Konfidenz, und 100 bedeutet 100 Prozent Konfidenz. Beispielsweise hat eine Erkennung einer Datenexfiltration, die auf einer statistischen Abweichung des Netzwerkverkehrs basiert, eine geringe Zuverlässigkeit, da eine tatsächliche Exfiltration nicht verifiziert wurde.

Beispiel

```
"Confidence": 42
```

Kritikalität

Der Grad der Wichtigkeit, der den Ressourcen zugewiesen wird, die mit einem Ergebnis verknüpft sind.

`Criticality`sollte nur durch Aufrufen der `BatchUpdateFindings`API-Operation aktualisiert werden. Aktualisieren Sie dieses Objekt nicht mit `BatchImportFindings`.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Criticality` sollten Sie das `Criticality` Attribut unter verwenden`FindingProviderFields`. Siehe the section called “Aktualisierung der Ergebnisse mit FindingProviderFields”.

`Criticality`wird auf einer Basis von 0—100 bewertet, wobei eine Verhältnisskala verwendet wird, die nur ganze Zahlen unterstützt. Ein Wert von 0 bedeutet, dass die zugrunde liegenden Ressourcen keine Kritikalität haben, und der Wert 100 ist den wichtigsten Ressourcen vorbehalten.

Beachten Sie bei der Zuweisung für jede Ressource Folgendes: `Criticality`

- Enthält die betroffene Ressource sensible Daten (z. B. einen S3-Bucket mit PII)?

- Ermöglicht die betroffene Ressource einem Angreifer, seinen Zugriff zu vertiefen oder seine Fähigkeiten zur Ausführung zusätzlicher bösartiger Aktivitäten auszuweiten (z. B. ein kompromittiertes Systemadministratorkonto)?
- Ist die Ressource ein geschäftskritisches Asset (z. B. ein wesentliches Unternehmenssystem, dessen Kompromittierung bedeutende Umsatzeinbußen verursachen könnte)?

Sie können die folgenden Richtlinien verwenden:

- Eine Ressource, die geschäftskritische Systeme mit Strom versorgt oder hochsensible Daten enthält, kann im Bereich von 75 bis 100 bewertet werden.
- Eine Ressource, die wichtige (aber nicht kritische Systeme) mit Strom versorgt oder mäßig wichtige Daten enthält, kann im Bereich 25—74 bewertet werden.
- Eine Ressource, die unwichtige Systeme unterstützt oder unsensible Daten enthält, sollte im Bereich von 0—24 bewertet werden.

Beispiel

```
"Criticality": 99
```

Erkennung

Das `Detection` Objekt enthält Details zu einer Angriffssequenz, die von Amazon GuardDuty Extended Threat Detection gefunden wurde. GuardDuty generiert eine Erkennung der Angriffssequenz, wenn mehrere Ereignisse auf eine potenziell verdächtige Aktivität zurückzuführen sind. Um die Ergebnisse der GuardDuty Angriffssequenz in AWS Security Hub CSPM zu erhalten, müssen Sie die GuardDuty Aktivierung in Ihrem Konto aktiviert haben. Weitere Informationen finden Sie unter Amazon GuardDuty Extended Threat Detection im GuardDuty Amazon-Benutzerhandbuch.

Beispiel

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
```

```
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
       },
       "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "AROA987654321EXAMPLE:i-b188560f",
        "Account": {
         "Uid": "AccountId",
         "Name": "AccountName"
        }
       }
      }],
      "Endpoints": [{
       "Id": "EndpointId",
       "Ip": "203.0.113.1",
       "Domain": "example.com",
       "Port": 4040,
       "Location": {
        "City": "New York",
        "Country": "US",
        "Lat": 40.7123,
        "Lon": -74.0068
       },
       "AutonomousSystem": {
        "Name": "AnyCompany",
        "Number": 64496
       },
       "Connection": {
        "Direction": "INBOUND"
       }
      }],
      "Signals": [{
       "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
       "Title": "Someone ran a penetration test tool on your account.",
       "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
       "Count": 19,
       "FirstSeenAt": 1716916943000,
       "SignalIndicators": [
        {
         "Key": "ATTACK_TACTIC",
         "Title": "Attack Tactic",
```

```
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Data Destruction"
        ]
       },
      ],
      "LastSeenAt": 1716916944000,
      "Name": "Test:IAMUser/KaliLinux",
      "ResourceIds": [
       "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ],
      "Type": "FINDING"
     }],
     "SequenceIndicators": [
      {
       "Key": "ATTACK_TACTIC",
       "Title": "Attack Tactic",
       "Values": [
        "Discovery",
        "Exfiltration",
        "Impact"
       ]
      },
      {
       "Key": "HIGH_RISK_API",
       "Title": "High Risk Api",
       "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets"
        "s3:ListObjects"
```

```
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Cloud Service Discovery",
         "Data Destruction"
        ]
       }
      ]
     }
}
```

FindingProviderFields

`FindingProviderFields`umfasst die folgenden Attribute:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Die obigen Felder sind unter dem `FindingProviderFields` Objekt verschachtelt, haben jedoch Entsprechungen mit demselben Namen wie ASFF-Felder der obersten Ebene. Wenn ein neuer Befund von einem Suchprovider an Security Hub CSPM gesendet wird, füllt Security Hub CSPM das `FindingProviderFields` Objekt automatisch auf, wenn es aufgrund der entsprechenden Felder der obersten Ebene leer ist.

Finding Provider können Updates `FindingProviderFields` mithilfe der `BatchImportFindings`Security Hub CSPM-API aktualisieren. Die Suche nach Anbietern kann dieses Objekt nicht mit aktualisieren. `BatchUpdateFindings`

Einzelheiten darüber, wie Security Hub CSPM Updates von `BatchImportFindings` zu `FindingProviderFields` und zu den entsprechenden Attributen der obersten Ebene verarbeitet, finden Sie unter. the section called “Aktualisierung der Ergebnisse mit FindingProviderFields”

Kunden können die Felder der obersten Ebene mithilfe des Vorgangs aktualisieren. `BatchUpdateFindings` Kunden können nicht aktualisieren`FindingProviderFields`.

Beispiel

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder das Ereignis, das durch einen Befund erfasst wurde, zum ersten Mal beobachtet wurde.

Dieser Zeitstempel gibt an, wann das Ereignis oder die Sicherheitsanfälligkeit zum ersten Mal beobachtet wurde. Folglich kann er vom `CreatedAt` Zeitstempel abweichen, der angibt, wann dieser Ergebnisdatensatz erstellt wurde.

Bei Kontrollergebnissen, die Security Hub CSPM generiert und aktualisiert, kann dieser Zeitstempel auch angeben, wann sich der Compliance-Status einer Ressource zuletzt geändert hat. Bei anderen Arten von Ergebnissen sollte dieser Zeitstempel zwischen Aktualisierungen des Ergebnisdatensatzes unveränderlich sein. Er kann jedoch aktualisiert werden, wenn ein genauerer Zeitstempel ermittelt wird.

Beispiel

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder Ereignis, das durch einen Befund erfasst wurde, zuletzt vom Produkt mit Sicherheitsergebnissen beobachtet wurde.

Dieser Zeitstempel gibt an, wann das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde. Folglich kann er vom `UpdatedAt` Zeitstempel abweichen, der angibt, wann dieser Ergebnisdatensatz zuletzt oder zuletzt aktualisiert wurde.

Sie können diesen Zeitstempel angeben, er ist jedoch bei der ersten Beobachtung nicht erforderlich. Wenn Sie dieses Feld bei der ersten Beobachtung ausfüllen, sollte der Zeitstempel mit dem Zeitstempel identisch sein. `FirstObservedAt` Sie sollten dieses Feld immer wieder aktualisieren, sodass immer der Zeitstempel der letzten Beobachtung des Fundes angegeben wird.

Beispiel

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Schadsoftware

Das Objekt `Malware` stellt eine Liste der Malware zur Verfügung, die mit einem Fund zusammenhängt.

Beispiel

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Netzwerk (im Ruhestand)

Das `Network`Objekt stellt netzwerkbezogene Informationen zu einem Befund bereit.

Dieses Objekt ist ausgemustert. Um diese Daten bereitzustellen, können Sie die Daten entweder einer Ressource in zuordnen `Resources` oder das `Action` Objekt verwenden.

Beispiel

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
```

```
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

Das `NetworkPath`Objekt stellt Informationen über einen Netzwerkpfad bereit, der mit einem Befund zusammenhängt. Jeder Eintrag in `NetworkPath` steht für eine Komponente des Pfads.

Beispiel

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
```

```
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
     }
]
```

Hinweis

Das `Note`Objekt gibt eine benutzerdefinierte Notiz an, die Sie zu einem Ergebnis hinzufügen können.

Ein Ergebnisanbieter kann eine erste Notiz für ein Ergebnis bereitstellen, aber danach können keine Notizen hinzugefügt werden. Sie können eine Notiz nur mit `BatchUpdateFindings`aktualisieren.

Beispiel

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

Das `PatchSummary`Objekt bietet eine Zusammenfassung des Patch-Konformitätsstatus einer Instanz anhand eines ausgewählten Konformitätsstandards.

Beispiel

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
```

```
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Prozess

Das `Process`Objekt enthält prozessbezogene Details zu einem Ergebnis.

Beispiel:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Zeigt an, wann Security Hub CSPM ein Ergebnis erhalten hat und mit dessen Verarbeitung begonnen hat.

Dies unterscheidet sich von `CreatedAt` und`UpdatedAt`, bei denen es sich um erforderliche Zeitstempel handelt, die sich auf die Interaktion des Ermittlungsanbieters mit dem Sicherheitsproblem und dem Ergebnis beziehen. Der `ProcessedAt` Zeitstempel gibt an, wann Security Hub CSPM mit der Verarbeitung eines Ergebnisses beginnt. Nach Abschluss der Verarbeitung wird ein Ergebnis im Konto eines Benutzers angezeigt.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Ein Datentyp, bei dem Produkte mit Sicherheitsergebnissen zusätzliche lösungsspezifische Details enthalten können, die nicht Teil des definierten AWS Sicherheitsfindungsformats sind.

`ProductFields`Enthält Informationen zur Kontrolle für Ergebnisse, die von Security Hub CSPM-Kontrollen generiert wurden. Siehe the section called “Generierung und Aktualisierung von Kontrollergebnissen”.

Dieses Feld sollte keine redundanten Daten enthalten und darf keine Daten enthalten, die mit Feldern im AWS Security Finding Format in Konflikt stehen.

Das Präfix `aws/` "" steht für einen reservierten Namespace, der nur für AWS Produkte und Dienstleistungen reserviert ist und darf nicht zusammen mit Ergebnissen aus Integrationen von Drittanbietern eingereicht werden.

Auch wenn dies nicht unbedingt erforderlich ist, sollten Produkte Feldnamen wir folgt formatieren: `company-id/product-id/field-name`. Dabei sollten die `company-id` und `product-id` den Angaben im `ProductArn` des Fundes entsprechen.

Die Felder, auf die verwiesen wird, `Archival` werden verwendet, wenn Security Hub CSPM ein vorhandenes Ergebnis archiviert. Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren und wenn Sie konsolidierte Kontrollergebnisse ein- oder ausschalten.

Dieses Feld kann auch Informationen über den Standard enthalten, der die Kontrolle beinhaltet, die zu dem Ergebnis geführt hat.

Beispiel

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Gibt den Namen des Produkts an, das den Befund generiert hat. Für Ergebnisse, die auf Kontrollen basieren, lautet der Produktname Security Hub CSPM.

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. `BatchImportFindings` `BatchUpdateFindings` Die Ausnahme ist, wenn Sie eine benutzerdefinierte Integration verwenden. Siehe the section called “Maßgeschneiderte Produktintegrationen”.

Wenn Sie die Security Hub CSPM-Konsole verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie dieses Attribut.

Wenn Sie die Security Hub CSPM-API verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie das `aws/securityhub/ProductName` Attribut unter. `ProductFields`

Security Hub CSPM synchronisiert diese beiden Attribute nicht.

RecordState

Stellt den Datensatzstatus eines Ergebnisses bereit.

Standardmäßig werden Funde als `ACTIVE` erachtet, wenn sie anfangs von einem Service generiert werden.

Der Status `ARCHIVED` gibt an, dass ein Fund nicht mehr sichtbar sein sollte. Archivierte Ergebnisse werden nicht sofort gelöscht. Sie können sie suchen, überprüfen und darüber berichten. Security Hub CSPM archiviert automatisch kontrollbasierte Ergebnisse, wenn die zugehörige Ressource gelöscht wird, die Ressource nicht existiert oder die Kontrolle deaktiviert ist.

`RecordState`ist für die Suche nach Anbietern vorgesehen und kann nur mithilfe dieses Vorgangs aktualisiert werden. `BatchImportFindings` Sie können es nicht mithilfe des `BatchUpdateFindings`Vorgangs aktualisieren.

Um den Status Ihrer Untersuchung zu einem Ergebnis nachzuverfolgen, verwenden Sie `Workflow`stattRecordState.

Wenn sich der Datensatzstatus von `ARCHIVED` zu `ACTIVE` ändert und der Workflow-Status des Ergebnisses `NOTIFIED` oder lautet`RESOLVED`, ändert Security Hub CSPM den Workflow-Status automatisch in. `NEW`

Beispiel

```
"RecordState": "ACTIVE"
```

Region

Gibt den Wert an, AWS-Region aus dem der Befund generiert wurde.

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. `BatchImportFindings``BatchUpdateFindings`

Beispiel

```
"Region": "us-west-2"
```

RelatedFindings

Stellt eine Liste von Ergebnissen bereit, die sich auf das aktuelle Ergebnis beziehen.

`RelatedFindings`sollte nur mit der `BatchUpdateFindings`API-Operation aktualisiert werden. Sie sollten dieses Objekt nicht mit aktualisieren `BatchImportFindings`.

Für `BatchImportFindings`Anfragen sollte die Suche nach Anbietern das `RelatedFindings` Objekt unter verwenden `FindingProviderFields`.

Beschreibungen der `RelatedFindings` Attribute finden Sie `RelatedFinding`in der AWS Security Hub API-Referenz.

Beispiel

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Beispiel

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
```

```
        "Indicators": [
            {
                "Type": "Reachability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            }
        ]
    }
}
```

Abhilfe

Das Objekt `Remediation` enthält Informationen zu empfohlenen Behebungsschritten für das Problem.

Beispiel

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 CSPM documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Beispiel

Gibt an, ob es sich bei dem Ergebnis um ein Beispielergebnis handelt.

```
"Sample": true
```

SourceUrl

Das `SourceUrl` Objekt stellt eine URL bereit, die auf eine Seite verweist, die sich mit dem aktuellen Ergebnis im gefundenen Produkt befasst.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

Das `ThreatIntelIndicator`Objekt stellt Bedrohungsinformationen bereit, die sich auf einen Befund beziehen.

Beispiel

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
```

```
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Bedrohungen

Das Threats-Objekt enthält Details zu der Bedrohung, die durch einen Befund erkannt wurde.

Beispiel

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Stellt eine Liste von Zeichenfolgenpaaren aus Name und Wert bereit, die dem Befund zugeordnet sind. Dies sind individuelle, benutzerdefinierte Felder, die einem Fund hinzugefügt werden. Diese Felder können anhand Ihrer spezifischen Konfiguration automatisch generiert werden.

Bei der Suche nach Anbietern sollte dieses Feld nicht für Daten verwendet werden, die das Produkt generiert. Stattdessen kann das `ProductFields` Feld bei der Suche nach Anbietern für Daten verwendet werden, die keinem Standardfeld im Format für AWS Sicherheitssuche zugeordnet sind.

Diese Felder können nur mit `BatchUpdateFindings` aktualisiert werden.

Beispiel

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Stellt den Wahrheitsgehalt eines Ergebnisses sicher. Finds-Produkte können `UNKNOWN` für dieses Feld einen Wert von angeben. Ein Ergebnisprodukt sollte einen Wert für dieses Feld liefern, wenn das System des Ergebnisprodukts ein aussagekräftiges Analogon enthält. Dieses Feld wird in der Regel durch eine Benutzerentscheidung oder eine Aktion nach der Untersuchung eines Ergebnisses gefüllt.

Ein Ergebnisanbieter kann einen Anfangswert für dieses Attribut bereitstellen, es danach aber nicht aktualisieren. Sie können dieses Attribut nur aktualisieren, indem Sie `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Schwachstellen

Das Vulnerabilities Objekt enthält eine Liste von Sicherheitslücken, die mit einem Befund verknüpft sind.

Beispiel

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
```

```
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Workflow

Das `Workflow`-Objekt bietet Informationen über den Status der Untersuchung zu einem Ergebnis.

Dieses Feld ist für Kunden zur Verwendung mit Tools zur Problembehebung, Orchestrierung und Ticketausstellung vorgesehen. Es ist nicht für die Suche nach Anbietern bestimmt.

Sie können das Feld nur mit aktualisieren. `Workflow` `BatchUpdateFindings` Kunden können ihn auch über die Konsole aktualisieren. Siehe the section called “Den Workflow-Status von Ergebnissen festlegen”.

Beispiel

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Im Ruhestand)

Dieses Objekt ist ausgemustert und wurde durch das `Status` Feld des `Workflow` Objekts ersetzt.

Dieses Feld gibt den Workflow-Status eines Ergebnisses an. Funde generierende Produkte können in diesem Feld den Wert `NEW` angeben. Ein Funde generierendes Produkte kann einen Wert in diesem Feld angeben, wenn es ein aussagekräftiges Analogon im System des Produkts gibt.

Beispiel

```
"WorkflowState": "NEW"
```

Ressourcen ASFF-Objekt

Im AWS Security Finding Format (ASFF) stellt das `Resources` Objekt Informationen zu den Ressourcen bereit, die an einem Befund beteiligt waren. Es enthält ein Array von bis zu 32 Ressourcenobjekten. Informationen zur Formatierung von Ressourcennamen finden Sie unterAWS Format für Sicherheitssuche (ASFF). Beispiele für jedes Ressourcenobjekt finden Sie, wenn Sie eine Ressource aus der folgenden Liste auswählen.

Themen

- Ressourcenattribute im ASFF
- AwsAmazonMQ Ressourcen in ASFF
- AwsApiGateway Ressourcen in ASFF
- AwsAppSync Ressourcen in ASFF

- AwsAthena Ressourcen in ASFF
- AwsAutoScaling Ressourcen in ASFF
- AwsBackup Ressourcen in ASFF
- AwsCertificateManager Ressourcen in ASFF
- AwsCloudFormation Ressourcen in ASFF
- AwsCloudFront Ressourcen in ASFF
- AwsCloudTrail Ressourcen in ASFF
- AwsCloudWatch Ressourcen in ASFF
- AwsCodeBuild Ressourcen in ASFF
- AwsDms Ressourcen in ASFF
- AwsDynamoDB Ressourcen in ASFF
- AwsEc2 Ressourcen in ASFF
- AwsEcr Ressourcen in ASFF
- AwsEcs Ressourcen in ASFF
- AwsEfs Ressourcen in ASFF
- AwsEks Ressourcen in ASFF
- AwsElasticBeanstalk Ressourcen in ASFF
- AwsElasticSearch Ressourcen in ASFF
- AwsElb Ressourcen in ASFF
- AwsEventBridge Ressourcen in ASFF
- AwsGuardDuty Ressourcen in ASFF
- AwsIam Ressourcen in ASFF
- AwsKinesis Ressourcen in ASFF
- AwsKms Ressourcen in ASFF
- AwsLambda
- AwsMsk Ressourcen in ASFF
- AwsNetworkFirewall Ressourcen in ASFF
- AwsOpenSearchService Ressourcen in ASFF
- AwsRds Ressourcen in ASFF
- AwsRedshift Ressourcen in ASFF

- AwsRoute53 Ressourcen in ASFF
- AWSS3 Ressourcen in ASFF
- AwsSageMaker Ressourcen in ASFF
- AwsSecretsManager Ressourcen in ASFF
- AwsSns Ressourcen in ASFF
- AwsSqs Ressourcen in ASFF
- AwsSsm Ressourcen in ASFF
- AwsStepFunctions Ressourcen in ASFF
- AwsWaf Ressourcen in ASFF
- AwsXray Ressourcen in ASFF
- CodeRepository Objekt in ASFF
- Behälter Objekt in ASFF
- Sonstige Objekt in ASFF

Ressourcenattribute im ASFF

Hier finden Sie Beschreibungen und Beispiele für das `Resources` Objekt im AWS Security Finding Format (ASFF). Weitere Informationen zu diesen Feldern finden Sie unter Ressourcen.

ApplicationArn

Identifiziert den Amazon-Ressourcennamen (ARN) der Anwendung, die an der Suche beteiligt war.

Beispiel

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifiziert den Namen der Anwendung, die an der Entdeckung beteiligt war.

Beispiel

```
"ApplicationName": "SampleApp"
```

DataClassification

Das DataClassificationFeld enthält Informationen über vertrauliche Daten, die auf der Ressource erkannt wurden.

Beispiel

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
```

```
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                 },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
```

```
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Details

Das Details Feld enthält zusätzliche Informationen über eine einzelne Ressource, die die entsprechenden Objekte verwendet. Jede Ressource muss in einem separaten Ressourcenobjekt im `Resources` Objekt bereitgestellt werden.

Beachten Sie, dass das `Details` Objekt aus dem Ergebnis entfernt wird, wenn die Ergebnisgröße das Maximum von 240 KB überschreitet. Für Kontrollergebnisse, die AWS Config Regeln verwenden, können Sie sich die Ressourcendetails in der AWS Config Konsole ansehen.

Security Hub CSPM bietet eine Reihe verfügbarer Ressourcendetails für die unterstützten Ressourcentypen. Diese Details entsprechen den Werten des `Type` Objekts. Verwenden Sie nach Möglichkeit die bereitgestellten Typen.

Wenn es sich bei der Ressource beispielsweise um einen S3-Bucket handelt, legen Sie die Ressource `Type` auf fest `AwsS3Bucket` und geben Sie die Ressourcendetails im `AwsS3Bucket` Objekt an.

Mit dem `Other` Objekt können Sie benutzerdefinierte Felder und Werte angeben. Sie verwenden das `Other` Objekt in den folgenden Fällen:

- Der Ressourcentyp (der Wert der ResourceType) hat kein entsprechendes Detailobjekt. Um Details für die Ressource bereitzustellen, verwenden Sie das `Other` Objekt.
- Das Objekt für den Ressourcentyp enthält nicht alle Felder, die Sie auffüllen möchten. Verwenden Sie in diesem Fall das Detailobjekt für den Ressourcentyp, um die verfügbaren Felder auszufüllen.

Verwenden Sie das `Other` Objekt, um die Felder aufzufüllen, die sich nicht im typspezifischen Objekt befinden.

- Der Ressourcentyp gehört nicht zu den angegebenen Typen. Stellen Sie in diesem Fall `Resource.Type` auf ein und verwenden Sie das `Other` Objekt`Other`, um die Details aufzufüllen.

Beispiel

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

Der Bezeichner für den angegebenen Ressourcentyp.

Für AWS Ressourcen, die durch Amazon Resource Names (ARNs) identifiziert werden, ist dies der ARN.

Für AWS Ressourcen, denen ARNs fehlen, ist dies die Kennung, wie sie von dem AWS Service definiert wurde, der die Ressource erstellt hat.

Bei AWS Nicht-Ressourcen ist dies eine eindeutige Kennung, die der Ressource zugeordnet ist.

Beispiel

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

Die Partition, in der sich die Ressource befindet. Eine Partition ist eine Gruppe von AWS-Regionen. Jede AWS-Konto ist auf eine Partition beschränkt.

Die folgenden Partitionen werden unterstützt:

- `aws` – AWS-Regionen
- `aws-cn` – China-Regionen
- `aws-us-gov` – AWS GovCloud (US) Region

Beispiel

```
"Partition": "aws"
```

Region

Der Code für den AWS-Region Ort, an dem sich diese Ressource befindet. Eine Liste der Regionscodes finden Sie unter Regionale Endpunkte.

Beispiel

```
"Region": "us-west-2"
```

ResourceRole

Identifiziert die Rolle der Ressource bei dem Ergebnis. Eine Ressource ist entweder das Ziel der Suchaktivität oder der Akteur, der die Aktivität ausgeführt hat.

Beispiel

```
"ResourceRole": "target"
```

Tags (Markierungen)

Dieses Feld enthält Informationen zu Schlüsselwörtern und Werten für die Ressource, die an einem Ergebnis beteiligt war. Sie können Ressourcen taggen, die vom `GetResources` Betrieb der AWS - Ressourcengruppen Tagging-API unterstützt werden. Security Hub CSPM ruft diesen Vorgang über die dienstverknüpfte Rolle auf und ruft die Ressourcen-Tags ab, wenn das `Resource.Id` Feld AWS Security Finding Format (ASFF) mit dem Ressourcen-ARN gefüllt ist. AWS Ungültige Ressourcen-IDs werden ignoriert.

Sie können Ressourcen-Tags zu Ergebnissen hinzufügen, die Security Hub CSPM aufnimmt, einschließlich Ergebnissen aus integrierten Produkten AWS-Services und Produkten von Drittanbietern.

Wenn Sie Tags hinzufügen, erfahren Sie, welche Tags einer Ressource zum Zeitpunkt der Verarbeitung des Ergebnisses zugeordnet waren. Sie können das `Tags` Attribut nur für Ressourcen einbeziehen, denen ein Tag zugeordnet ist. Wenn eine Ressource keine zugeordneten Tags hat, beziehen Sie beim Fund kein `Tags`-Attribut mit ein.

Durch die Aufnahme von Ressourcen-Tags in die Ergebnisse entfällt die Notwendigkeit, Pipelines zur Datenanreicherung zu erstellen oder die Metadaten von Sicherheitsergebnissen manuell anzureichern. Sie können Tags auch verwenden, um Ergebnisse und Erkenntnisse zu suchen oder zu filtern und Automatisierungsregeln zu erstellen.

Informationen zu Einschränkungen, die für Tags gelten, finden Sie unter Einschränkungen und Anforderungen für die Benennung von Tags.

In diesem Feld können Sie nur Tags angeben, die auf einer AWS Ressource vorhanden sind. Verwenden Sie das Unterfeld „`Other`Details“, um Daten bereitzustellen, die nicht im AWS Security Finding Format definiert sind.

Beispiel

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Typ

Der Ressourcentyp, für den Sie Details angeben.

Verwenden Sie nach Möglichkeit einen der bereitgestellten Ressourcentypen, z. B. `AwsEc2Instance` oder `AwsS3Bucket`.

Wenn der Ressourcentyp keinem der angegebenen Ressourcentypen entspricht, legen Sie die Ressource `Type` auf `Other` fest und füllen Sie die `Other` Details im Unterfeld „Details“ aus.

Unterstützte Werte sind unter Ressourcen aufgeführt.

Beispiel

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsAmazonMQ` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsAmazonMQBroker

`AwsAmazonMQBroker`bietet Informationen über einen Amazon MQ-Broker, eine Message-Broker-Umgebung, die auf Amazon MQ ausgeführt wird.

Das folgende Beispiel zeigt den ASFF für das Objekt. `AwsAmazonMQBroker` Beschreibungen der `AwsAmazonMQBroker` Attribute finden Sie AwsAmazonMQBrokerin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
```

```
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsApiGateway` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsApiGatewayRestApi

Das `AwsApiGatewayRestApi` Objekt enthält Informationen über eine REST-API in Version 1 von Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayRestApi` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayRestApi` Attribute finden Sie AwsApiGatewayRestApiDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

Das `AwsApiGatewayStage` Objekt stellt Informationen zu einer Amazon API Gateway Gateway-Stufe der Version 1 bereit.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayStage` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayStage` Attribute finden Sie AwsApiGatewayStageDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
```

```
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
```

```
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

Das `AwsApiGatewayV2Api` Objekt enthält Informationen über eine API der Version 2 in Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Api` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Api` Attribute finden Sie AwsApiGatewayV2ApiDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
```

```
            "POST",
            "DELETE",
            "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage`enthält Informationen über eine Version 2-Stufe für Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Stage` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsApiGatewayV2StageDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
```

```
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsAppSync` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`bietet Informationen über eine AWS AppSync GraphQL-API, bei der es sich um ein Konstrukt der obersten Ebene für Ihre Anwendung handelt.

Das folgende Beispiel zeigt den ASFF für das Objekt. `AwsAppSyncGraphQLApi` Beschreibungen der `AwsAppSyncGraphQLApi` Attribute finden Sie AwsAppSyncGraphQLApiin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAppSyncGraphQLApi": {
```

```
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsAthena` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`bietet Informationen über eine Amazon Athena Athena-Arbeitsgruppe. Eine Arbeitsgruppe hilft Ihnen dabei, Benutzer, Teams, Anwendungen oder Workloads voneinander zu trennen. Sie hilft Ihnen auch dabei, Grenzen für die Datenverarbeitung festzulegen und die Kosten nachzuverfolgen.

Das folgende Beispiel zeigt den ASFF für das `AwsAthenaWorkGroup` Objekt. Beschreibungen der `AwsAthenaWorkGroup` Attribute finden Sie AwsAthenaWorkGroupin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsAutoScaling` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsAutoScalingAutoScalingGroup

Das `AwsAutoScalingAutoScalingGroup` Objekt enthält Details zu einer automatischen Skalierungsgruppe.

Im Folgenden finden Sie ein Beispiel für einen `AwsAutoScalingAutoScalingGroup` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsAutoScalingAutoScalingGroup` Attribute finden Sie AwsAutoScalingAutoScalingGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAutoScalingAutoScalingGroup": {
```

```
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

Das `AwsAutoScalingLaunchConfiguration` Objekt enthält Details zu einer Startkonfiguration.

Im Folgenden finden Sie ein Beispiel für einen `AwsAutoScalingLaunchConfiguration` Befund im AWS Security Finding Format (ASFF).

Beschreibungen der `AwsAutoScalingLaunchConfiguration` Attribute finden Sie AwsAutoScalingLaunchConfigurationDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
```

```
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsBackup` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsBackupBackupPlan

Das `AwsBackupBackupPlan` Objekt stellt Informationen zu einem AWS Backup Backup-Plan bereit. Ein AWS Backup Backup-Plan ist ein Richtlinienausdruck, der definiert, wann und wie Sie Ihre AWS Ressourcen sichern möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupBackupPlan` Objekt. Beschreibungen der `AwsBackupBackupPlan` Attribute finden Sie AwsBackupBackupPlanin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
```

```
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
```

```
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

Das `AwsBackupBackupVault` Objekt stellt Informationen zu einem AWS Backup Backup-Tresor bereit. Ein AWS Backup Backup-Tresor ist ein Container, der Ihre Backups speichert und organisiert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupBackupVault` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie AwsBackupBackupVaultin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
```

```
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

Das `AwsBackupRecoveryPoint` Objekt stellt Informationen zu einer AWS Backup Sicherung bereit, die auch als Wiederherstellungspunkt bezeichnet wird. Ein AWS Backup Wiederherstellungspunkt stellt den Inhalt einer Ressource zu einem bestimmten Zeitpunkt dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupRecoveryPoint` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie AwsBackupRecoveryPointin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
```

```
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

AwsCertificateManager Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCertificateManager` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCertificateManagerCertificate

Das `AwsCertificateManagerCertificate` Objekt enthält Details zu einem AWS Certificate Manager (ACM-) Zertifikat.

Im Folgenden finden Sie ein Beispiel für einen `AwsCertificateManagerCertificate` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCertificateManagerCertificate` Attribute finden Sie AwsCertificateManagerCertificateDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
```

```
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
```

```
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCloudFormation` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCloudFormationStack

Das `AwsCloudFormationStack` Objekt enthält Details zu einem AWS CloudFormation Stapel, der als Ressource in einer Vorlage der obersten Ebene verschachtelt ist.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsCloudFormationStack` Beschreibungen der `AwsCloudFormationStack` Attribute finden Sie AwsCloudFormationStackDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```


AwsCloudFront Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCloudFront` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCloudFrontDistribution

Das `AwsCloudFrontDistribution` Objekt enthält Details zu einer CloudFront Amazon-Vertriebskonfiguration.

Im Folgenden finden Sie ein Beispiel für einen `AwsCloudFrontDistribution` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCloudFrontDistribution` Attribute finden Sie AwsCloudFrontDistributionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
                              301,
                              404
                          ]
                          "Quantity": 3
                      }
                 }
              }
           ]
     },
```

```
     "Origins": {
           "Items": [
               {
                  "CustomOriginConfig": {
                      "HttpPort": 80,
                      "HttpsPort": 443,
                      "OriginKeepaliveTimeout": 60,
                      "OriginProtocolPolicy": "match-viewer",
                      "OriginReadTimeout": 30,
                      "OriginSslProtocols": {
                        "Items": ["SSLv3", "TLSv1"],
                        "Quantity": 2
                      }
                  }
               },
           ]
     },
                  "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                  "Id": "my-origin",
                  "OriginPath": "/production",
                  "S3OriginConfig": {
                      "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                  }
           ]
     },
     "Status": "Deployed",
     "ViewerCertificate": {
            "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
            "Certificate": "ASCAJRRE5XYF52TKRY5M4",
            "CertificateSource": "iam",
            "CloudFrontDefaultCertificate": true,
            "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
            "MinimumProtocolVersion": "TLSv1.2_2021",
            "SslSupportMethod": "sni-only"
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCloudTrail` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCloudTrailTrail

Das `AwsCloudTrailTrail` Objekt liefert Details zu einer AWS CloudTrail Spur.

Im Folgenden finden Sie ein Beispiel für einen `AwsCloudTrailTrail` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCloudTrailTrail` Attribute finden Sie AwsCloudTrailTrailDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCloudWatch` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCloudWatchAlarm

Das `AwsCloudWatchAlarm` Objekt bietet Details zu CloudWatch Amazon-Alarmen, die eine Metrik beobachten oder eine Aktion ausführen, wenn sich der Status eines Alarms ändert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsCloudWatchAlarm` Objekt. Beschreibungen der `AwsCloudWatchAlarm` Attribute finden Sie AwsCloudWatchAlarmDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
```

```
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsCodeBuild` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsCodeBuildProject

Das Objekt `AwsCodeBuildProject` liefert Informationen zu einem AWS CodeBuild -Projekt.

Im Folgenden finden Sie ein Beispiel für einen `AwsCodeBuildProject` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCodeBuildProject` Attribute finden Sie AwsCodeBuildProjectDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
```

```
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
             "Status": "string",
             "StreamName": "string"
        },
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
   },
   "Name": "string",
   "ServiceRole": "string",
   "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
   },
   "VpcConfig": {
        "VpcId": "string",
```

```
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}
```

AwsDms Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsDms` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsDmsEndpoint

Das `AwsDmsEndpoint` Objekt stellt Informationen über einen AWS Database Migration Service (AWS DMS) -Endpunkt bereit. Ein Endpunkt stellt Verbindungs-, Datenspeichertyp- und Standortinformationen zu Ihrem Datenspeicher bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsEndpoint` Objekt. Beschreibungen der `AwsDmsEndpoint` Attribute finden Sie AwsDmsEndpointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

Das `AwsDmsReplicationInstance` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsinstanz bereit. DMS verwendet eine Replikationsinstanz, um eine Verbindung zu Ihrem Quelldatenspeicher herzustellen, die Quelldaten zu lesen und die Daten für den Zieldatenspeicher zu formatieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie AwsDmsReplicationInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

Das `AwsDmsReplicationTask` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsaufgabe bereit. Eine Replikationsaufgabe verschiebt einen Datensatz vom Quellendpunkt zum Zielendpunkt.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie AwsDmsReplicationInstancein der AWS Security Hub API-Referenz.

Beispiel


```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
```

```
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```


AwsDynamoDB Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für Ressourcen. `AwsDynamoDB`

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsDynamoDbTable

Das `AwsDynamoDbTable` Objekt enthält Details zu einer Amazon DynamoDB-Tabelle.

Im Folgenden finden Sie ein Beispiel für einen `AwsDynamoDbTable` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsDynamoDbTable` Attribute finden Sie AwsDynamoDbTableDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
```

```
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
```

```
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
```

```
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2 Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEc2` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEc2ClientVpnEndpoint

Das `AwsEc2ClientVpnEndpoint` Objekt stellt Informationen über einen AWS Client VPN Endpunkt bereit. Ein Client-VPN-Endpunkt ist die Ressource, die Sie erstellen und konfigurieren, um Client-VPN-Sitzungen zu aktivieren und zu verwalten. Es handelt sich hier um den Beendigungspunkt für alle Client-VPN-Sitzungen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2ClientVpnEndpoint` Objekt. Beschreibungen der `AwsEc2ClientVpnEndpoint` Attribute finden Sie AwsEc2ClientVpnEndpointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
```

```
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

Das `AwsEc2Eip` Objekt stellt Informationen über eine Elastic IP-Adresse bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Eip` Objekt. Beschreibungen der `AwsEc2Eip` Attribute finden Sie AwsEc2EipDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

Das `AwsEc2Instance` Objekt enthält Details zu einer Amazon EC2 EC2-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Instance` Objekt. Beschreibungen der `AwsEc2Instance` Attribute finden Sie AwsEc2InstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

Das `AwsEc2LaunchTemplate` Objekt enthält Details zu einer Amazon Elastic Compute Cloud-Startvorlage, die Informationen zur Instance-Konfiguration spezifiziert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2LaunchTemplate` Objekt. Beschreibungen der `AwsEc2LaunchTemplate` Attribute finden Sie AwsEc2LaunchTemplateDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

Das `AwsEc2NetworkAcl` Objekt enthält Details zu einer Amazon EC2 EC2-Netzwerkzugriffskontrollliste (ACL).

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkAcl` Objekt. Beschreibungen der `AwsEc2NetworkAcl` Attribute finden Sie AwsEc2NetworkAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
   }]
}
```

AwsEc2NetworkInterface

Das `AwsEc2NetworkInterface` Objekt stellt Informationen über eine Amazon EC2 EC2-Netzwerkschnittstelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkInterface` Objekt. Beschreibungen der `AwsEc2NetworkInterface` Attribute finden Sie AwsEc2NetworkInterfaceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

Das `AwsEc2RouteTable` Objekt stellt Informationen über eine Amazon EC2 EC2-Routentabelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2RouteTable` Objekt. Beschreibungen der `AwsEc2RouteTable` Attribute finden Sie AwsEc2RouteTableDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
```

```
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

Das `AwsEc2SecurityGroup` Objekt beschreibt eine Amazon EC2-Sicherheitsgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2SecurityGroup` Objekt. Beschreibungen der `AwsEc2SecurityGroup` Attribute finden Sie AwsEc2SecurityGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
```

```
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

Das `AwsEc2Subnet` Objekt stellt Informationen über ein Subnetz in Amazon EC2 bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEc2Subnet` Beschreibungen der `AwsEc2Subnet` Attribute finden Sie AwsEc2SubnetDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
```

```
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

Das `AwsEc2TransitGateway` Objekt enthält Details zu einem Amazon EC2-Transit-Gateway, das Ihre virtuellen privaten Clouds (VPCs) und lokalen Netzwerke miteinander verbindet.

Im Folgenden finden Sie ein Beispiel für einen `AwsEc2TransitGateway` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsEc2TransitGateway` Attribute finden Sie AwsEc2TransitGatewayDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

Das `AwsEc2Volume` Objekt enthält Details zu einem Amazon EC2 EC2-Volume.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Volume` Objekt. Beschreibungen der `AwsEc2Volume` Attribute finden Sie AwsEc2VolumeDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

Das `AwsEc2Vpc` Objekt enthält Details zu einer Amazon EC2 EC2-VPC.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEc2Vpc` Beschreibungen der `AwsEc2Vpc` Attribute finden Sie AwsEc2VpcDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
```

```
            "Ipv6CidrBlock": "192.0.2.0/24"
        }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

Das `AwsEc2VpcEndpointService` Objekt enthält Details zur Dienstkonfiguration für einen VPC-Endpunktdienst.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpcEndpointService` Objekt. Beschreibungen der `AwsEc2VpcEndpointService` Attribute finden Sie AwsEc2VpcEndpointServiceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

Das `AwsEc2VpcPeeringConnection` Objekt enthält Details zur Netzwerkverbindung zwischen zwei VPCs.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpcPeeringConnection` Objekt. Beschreibungen der `AwsEc2VpcPeeringConnection` Attribute finden Sie AwsEc2VpcPeeringConnectionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
```

```
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEcr Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEcr` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEcrContainerImage

Das `AwsEcrContainerImage` Objekt stellt Informationen zu einem Amazon ECR-Bild bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrContainerImage` Objekt. Beschreibungen der `AwsEcrContainerImage` Attribute finden Sie AwsEcrContainerImageDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

Das `AwsEcrRepository` Objekt stellt Informationen über ein Amazon Elastic Container Registry-Repository bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrRepository` Objekt. Beschreibungen der `AwsEcrRepository` Attribute finden Sie AwsEcrRepositoryDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEcs` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEcsCluster

Das `AwsEcsCluster` Objekt enthält Details zu einem Amazon Elastic Container Service-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsCluster` Objekt. Beschreibungen der `AwsEcsCluster` Attribute finden Sie AwsEcsClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
```

```
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

Das `AwsEcsContainer` Objekt enthält Details zu einem Amazon ECS-Container.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsContainer` Objekt. Beschreibungen der `AwsEcsContainer` Attribute finden Sie AwsEcsContainerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

Das `AwsEcsService` Objekt bietet Details zu einem Service innerhalb eines Amazon ECS-Clusters.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsService` Objekt. Beschreibungen der `AwsEcsService` Attribute finden Sie AwsEcsServiceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
```

```
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

Das `AwsEcsTask` Objekt enthält Details zu einer Amazon ECS-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTask` Objekt. Beschreibungen der `AwsEcsTask` Attribute finden Sie AwsEcsTaskin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

Das `AwsEcsTaskDefinition` Objekt enthält Details zu einer Aufgabendefinition. Eine Aufgabendefinition beschreibt die Container- und Volume-Definitionen einer Amazon Elastic Container Service-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTaskDefinition` Objekt. Beschreibungen der `AwsEcsTaskDefinition` Attribute finden Sie AwsEcsTaskDefinitionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
```

```
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEfs` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEfsAccessPoint

Das `AwsEfsAccessPoint` Objekt enthält Details zu Dateien, die im Amazon Elastic File System gespeichert sind.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEfsAccessPoint` Objekt. Beschreibungen der `AwsEfsAccessPoint` Attribute finden Sie AwsEfsAccessPointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
```

```
    "OwnerUid": "1234",
    "Permissions": "777"
   },
   "Path": "/tmp/example"
  }
}
```

AwsEks Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEks` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEksCluster

Das `AwsEksCluster` Objekt enthält Details zu einem Amazon EKS-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEksCluster` Objekt. Beschreibungen der `AwsEksCluster` Attribute finden Sie AwsEksClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
```

```
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für Ressourcen. `AwsElasticBeanstalk`

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsElasticBeanstalkEnvironment

Das `AwsElasticBeanstalkEnvironment` Objekt enthält Details zu einer AWS Elastic Beanstalk Umgebung.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticBeanstalkEnvironment` Objekt. Beschreibungen der `AwsElasticBeanstalkEnvironment` Attribute finden Sie AwsElasticBeanstalkEnvironmentDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
```

```
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
```

```
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsElasticSearch` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsElasticSearchDomain

Das `AwsElasticSearchDomain` Objekt enthält Details zu einer Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticSearchDomain` Objekt. Beschreibungen der `AwsElasticSearchDomain` Attribute finden Sie AwsElasticSearchDomainDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
```

```
            "DedicatedMasterCount": number,
            "DedicatedMasterEnabled": boolean,
            "DedicatedMasterType": "string",
            "InstanceCount": number,
            "InstanceType": "string",
            "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
            },
            "ZoneAwarenessEnabled": boolean
      },
      "ElasticsearchVersion": "string",
      "EncryptionAtRestOptions": {
            "Enabled": boolean,
            "KmsKeyId": "string"
      },
      "LogPublishingOptions": {
            "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            }
      },
      "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
      },
      "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
      },
      "VPCOptions": {
            "AvailabilityZones": [
                  "string"
```

```
            ],
            "SecurityGroupIds": [
                  "string"
            ],
            "SubnetIds": [
                  "string"
            ],
           "VPCId": "string"
    }
}
```

AwsElb Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsElb` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsElbLoadBalancer

Das `AwsElbLoadBalancer` Objekt enthält Details zu einem Classic Load Balancer.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbLoadBalancer` Objekt. Beschreibungen der `AwsElbLoadBalancer` Attribute finden Sie AwsElbLoadBalancerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
```

```
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "amzn-s3-demo-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]
```

```
    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

Das Objekt `AwsElbv2LoadBalancer` stellt Informationen über einen Load Balancer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbv2LoadBalancer` Objekt. Beschreibungen der `AwsElbv2LoadBalancer` Attribute finden Sie AwsElbv2LoadBalancerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
                        "Type": "string",
                        "VpcId": "string"
                    }
```

AwsEventBridge Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEventBridge` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsEventSchemasRegistry

Das `AwsEventSchemasRegistry` Objekt stellt Informationen über eine EventBridge Amazon-Schemaregistrierung bereit. Ein Schema definiert die Struktur der Ereignisse, an die gesendet werden EventBridge. Schemaregister sind Container, die Ihre Schemas sammeln und logisch gruppieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventSchemasRegistry` Beschreibungen der `AwsEventSchemasRegistry` Attribute finden Sie AwsEventSchemasRegistryin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

Das `AwsEventsEndpoint` Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpunkt bereit. Der Endpunkt kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie Regional-fault tolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEventsEndpoint` Objekt. Beschreibungen der `AwsEventsEndpoint` Attribute finden Sie AwsEventsEndpointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
```

```
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

Das `AwsEventsEventbus` Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpunkt bereit. Der Endpunkt kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie Regional-fault tolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEventsEventbus` Objekt. Beschreibungen der `AwsEventsEventbus` Attribute finden Sie AwsEventsEventbusDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid
\":\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule\",
\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsGuardDuty` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsGuardDutyDetector

Das `AwsGuardDutyDetector` Objekt liefert Informationen über einen GuardDuty Amazon-Detektor. Ein Detektor ist ein Objekt, das den GuardDuty Service repräsentiert. Ein Detektor ist erforderlich GuardDuty , um betriebsbereit zu sein.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsGuardDutyDetector` Objekt. Beschreibungen der `AwsGuardDutyDetector` Attribute finden Sie AwsGuardDutyDetectorin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
```

```
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsIam` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsIamAccessKey

Das `AwsIamAccessKey` Objekt enthält Details zu einem IAM-Zugriffsschlüssel, der sich auf einen Befund bezieht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamAccessKey` Objekt. Beschreibungen der `AwsIamAccessKey` Attribute finden Sie AwsIamAccessKeyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
```

```
                        },
                        "SessionIssuer": {
                            "AccountId": "string",
                            "Arn": "string",
                            "PrincipalId": "string",
                            "Type": "string",
                            "UserName": "string"
                        }
                    },
                    "Status": "string"
                }
```

AwsIamGroup

Das `AwsIamGroup` Objekt enthält Details zu einer IAM-Gruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamGroup` Objekt. Beschreibungen der `AwsIamGroup` Attribute finden Sie AwsIamGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

Das `AwsIamPolicy` Objekt stellt eine IAM-Berechtigungsrichtlinie dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamPolicy` Objekt. Beschreibungen der `AwsIamPolicy` Attribute finden Sie AwsIamPolicyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

Das `AwsIamRole` Objekt enthält Informationen zu einer IAM-Rolle, einschließlich aller Richtlinien der Rolle.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamRole` Objekt. Beschreibungen der `AwsIamRole` Attribute finden Sie AwsIamRoleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17',       'Statement':
 [{'Effect': 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
```

```
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

Das `AwsIamUser` Objekt stellt Informationen über einen Benutzer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamUser` Objekt. Beschreibungen der `AwsIamUser` Attribute finden Sie AwsIamUserDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsKinesis` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsKinesisStream

Das `AwsKinesisStream` Objekt enthält Details zu Amazon Kinesis Data Streams.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsKinesisStream` Objekt. Beschreibungen der `AwsKinesisStream` Attribute finden Sie AwsKinesisStreamDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsKms` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsKmsKey

Das `AwsKmsKey` Objekt enthält Details zu einem AWS KMS key.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsKmsKey` Objekt. Beschreibungen der `AwsKmsKey` Attribute finden Sie AwsKmsKeyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
```

```
                    "Description": "string",
                    "KeyId": "string",
                    "KeyManager": "string",
                    "KeyRotationStatus": boolean,
                    "KeyState": "string",
                    "Origin": "string"
                }
```

AwsLambda

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsLambda` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsLambdaFunction

Das `AwsLambdaFunction` Objekt enthält Details zur Konfiguration einer Lambda-Funktion.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaFunction` Objekt. Beschreibungen der `AwsLambdaFunction` Attribute finden Sie AwsLambdaFunctionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
```

```
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

Das `AwsLambdaLayerVersion` Objekt enthält Details zu einer Lambda-Layer-Version.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaLayerVersion` Objekt. Beschreibungen der `AwsLambdaLayerVersion` Attribute finden Sie AwsLambdaLayerVersionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsLambdaLayerVersion": {
    "Version": 2,
```

```
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsMsk` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsMskCluster

Das `AwsMskCluster` Objekt stellt Informationen über einen Amazon Managed Streaming for Apache Kafka (Amazon MSK) -Cluster bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsMskCluster` Beschreibungen der `AwsMskCluster` Attribute finden Sie AwsMskClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
```

```
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsNetworkFirewall` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsNetworkFirewallFirewall

Das `AwsNetworkFirewallFirewall` Objekt enthält Details zu einer AWS Network Firewall Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewall` Objekt. Beschreibungen der `AwsNetworkFirewallFirewall` Attribute finden Sie AwsNetworkFirewallFirewallDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
```

```
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

Das `AwsNetworkFirewallFirewallPolicy` Objekt enthält Details zu einer Firewall-Richtlinie. Eine Firewall-Richtlinie definiert das Verhalten einer Netzwerk-Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewallPolicy` Objekt. Beschreibungen der `AwsNetworkFirewallFirewallPolicy` Attribute finden Sie AwsNetworkFirewallFirewallPolicyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
```

```
      ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

Das `AwsNetworkFirewallRuleGroup` Objekt enthält Details zu einer AWS Network Firewall Regelgruppe. Regelgruppen werden verwendet, um den Netzwerkverkehr zu untersuchen und zu kontrollieren. Zustandslose Regelgruppen gelten für einzelne Pakete. Stateful-Regelgruppen gelten für Pakete im Kontext ihres Datenverkehrs.

Auf Regelgruppen wird in Firewallrichtlinien verwiesen.

Die folgenden Beispiele zeigen das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallRuleGroup` Objekt. Beschreibungen der `AwsNetworkFirewallRuleGroup` Attribute finden Sie AwsNetworkFirewallRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel — Regelgruppe ohne Status

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
```

```
                            "aws:pass"
                        ],
                        "MatchAttributes": {
                            "DestinationPorts": [
                                {
                                    "FromPort": 443,
                                    "ToPort": 443
                                }
                            ],
                            "Destinations": [
                                {
                                    "AddressDefinition": "192.0.2.0/24"
                                }
                            ],
                            "Protocols": [
                                       6
                            ],
                            "SourcePorts": [
                                {
                                    "FromPort": 0,
                                    "ToPort": 65535
                                }
                            ],
                            "Sources": [
                                {
                                     "AddressDefinition": "198.51.100.0/24"
                                }
                            ]
                        }
                    }
                }
            ]
        }
    }
}
```

Beispiel — Regelgruppe mit Status

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
```

```
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
            "StatefulRules": [
                {
                    "Action": "PASS",
                    "Header": {
                        "Destination": "Any",
                        "DestinationPort": "443",
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
         }
    }
}
```

Die folgende Liste enthält Beispiele für gültige Werte für `AwsNetworkFirewallRuleGroup` Attribute:

- `Action`

  Zulässige Werte: `PASS` | `DROP` | `ALERT`

- `Protocol`

  Gültige Werte: `IP` `TCP` | `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` | `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | `DHCP`

- `Flags`

  Zulässige Werte: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

- `Masks`

Zulässige Werte: `FIN | SYN | RST | PSH | ACK | URG | ECE | CWR`

AwsOpenSearchService Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsOpenSearchService` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsOpenSearchServiceDomain

Das `AwsOpenSearchServiceDomain` Objekt enthält Informationen über eine Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsOpenSearchServiceDomain` Objekt. Beschreibungen der `AwsOpenSearchServiceDomain` Attribute finden Sie AwsOpenSearchServiceDomainDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
```

```
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
```

```
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsRds` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsRdsDbCluster

Das `AwsRdsDbCluster` Objekt enthält Details zu einem Amazon RDS-Datenbankcluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbCluster` Objekt. Beschreibungen der `AwsRdsDbCluster` Attribute finden Sie AwsRdsDbClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
```

```
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
```

```
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

Das `AwsRdsDbClusterSnapshot` Objekt enthält Informationen über einen Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbClusterSnapshot` Objekt. Beschreibungen der `AwsRdsDbClusterSnapshot` Attribute finden Sie AwsRdsDbClusterSnapshotDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
```

```
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

Das `AwsRdsDbInstance` Objekt enthält Details zu einer Amazon RDS-DB-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbInstance` Objekt. Beschreibungen der `AwsRdsDbInstance` Attribute finden Sie AwsRdsDbInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
```

```
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
```

```
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
```

```
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

Das `AwsRdsDbSecurityGroup` Objekt enthält Informationen über einen Amazon Relational Database Service

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSecurityGroup` Objekt. Beschreibungen der `AwsRdsDbSecurityGroup` Attribute finden Sie AwsRdsDbSecurityGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
```

```
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

Das `AwsRdsDbSnapshot` Objekt enthält Details zu einem Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSnapshot` Objekt. Beschreibungen der `AwsRdsDbSnapshot` Attribute finden Sie AwsRdsDbSnapshotDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
```

```
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

Das `AwsRdsEventSubscription` enthält Einzelheiten zu einem Abonnement für RDS-Ereignisbenachrichtigungen. Das Abonnement ermöglicht es RDS, Ereignisse zu einem SNS-Thema zu veröffentlichen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsEventSubscription` Objekt. Beschreibungen der `AwsRdsEventSubscription` Attribute finden Sie AwsRdsEventSubscriptionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsRedshift` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsRedshiftCluster

Das `AwsRedshiftCluster` Objekt enthält Details zu einem Amazon Redshift Redshift-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRedshiftCluster` Objekt. Beschreibungen der `AwsRedshiftCluster` Attribute finden Sie AwsRedshiftClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
```

```
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
```

```
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
```

```
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "amzn-s3-demo-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
```

```
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53 Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsRoute53` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsRoute53HostedZone

Das `AwsRoute53HostedZone` Objekt stellt Informationen über eine von Amazon Route 53 gehostete Zone bereit, einschließlich der vier Nameserver, die der Hosting-Zone zugewiesen sind. Eine gehostete Zone stellt eine Sammlung von Datensätzen dar, die zusammen verwaltet werden können und zu einem einzigen übergeordneten Domainnamen gehören.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRoute53HostedZone` Objekt. Beschreibungen der `AwsRoute53HostedZone` Attribute finden Sie AwsRoute53HostedZoneDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AWSS3 Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsS3` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsS3AccessPoint

`AwsS3AccessPoint`bietet Informationen über einen Amazon S3 S3-Zugriffspunkt. S3-Zugriffspunkte sind benannte Netzwerkendpunkte, die an S3-Buckets angeschlossen sind, mit denen Sie S3-Objektoperationen ausführen können.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsS3AccessPoint` Beschreibungen der `AwsS3AccessPoint` Attribute finden Sie AwsS3AccessPointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "amzn-s3-demo-bucket",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock`bietet Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3AccountPublicAccessBlock` Objekt. Beschreibungen der `AwsS3AccountPublicAccessBlock` Attribute finden Sie AwsS3AccountPublicAccessBlockDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

Das `AwsS3Bucket` Objekt enthält Details zu einem Amazon S3 S3-Bucket.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Bucket` Objekt. Beschreibungen der `AwsS3Bucket` Attribute finden Sie AwsS3BucketDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
```

```
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-123456789012",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
    "FilterRules": [
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
     "Value": "pre"
    },
```

```
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
         "Value": "suf"
        },
        ]
       }
      },
      "Type": "LambdaConfiguration"
     }]
    },
    "BucketVersioningConfiguration": {
     "IsMfaDeleteEnabled": true,
     "Status": "Off"
    },
    "BucketWebsiteConfiguration": {
     "ErrorDocument": "error.html",
     "IndexDocumentSuffix": "index.html",
     "RedirectAllRequestsTo": {
      "HostName": "example.com",
      "Protocol": "http"
     },
     "RoutingRules": [{
      "Condition": {
       "HttpErrorCodeReturnedEquals": "Redirected",
       "KeyPrefixEquals": "index"
         },
      "Redirect": {
       "HostName": "example.com",
       "HttpRedirectCode": "401",
       "Protocol": "HTTP",
       "ReplaceKeyPrefixWith": "string",
       "ReplaceKeyWith": "string"
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
```

```
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

Ein WSS3-Objekt

Das `AwsS3Object` Objekt stellt Informationen über ein Amazon S3 S3-Objekt bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Object` Objekt. Beschreibungen der `AwsS3Object` Attribute finden Sie AwsS3ObjectDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSageMaker` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsSageMakerNotebookInstance

Das `AwsSageMakerNotebookInstance` Objekt stellt Informationen über eine Amazon SageMaker AI-Notebook-Instance bereit, bei der es sich um eine Recheninstanz für maschinelles Lernen handelt, auf der die Jupyter Notebook App ausgeführt wird.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsSageMakerNotebookInstance` Beschreibungen der `AwsSageMakerNotebookInstance` Attribute finden Sie AwsSageMakerNotebookInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
```

```
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSecretsManager` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsSecretsManagerSecret

Das `AwsSecretsManagerSecret` Objekt enthält Details zu einem Secrets Manager Manager-Geheimnis.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSecretsManagerSecret` Objekt. Beschreibungen der `AwsSecretsManagerSecret` Attribute finden Sie AwsSecretsManagerSecretDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSns` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsSnsTopic

Das `AwsSnsTopic` Objekt enthält Details zu einem Thema von Amazon Simple Notification Service.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSnsTopic` Objekt. Beschreibungen der `AwsSnsTopic` Attribute finden Sie AwsSnsTopicDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSqs` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsSqsQueue

Das `AwsSqsQueue` Objekt enthält Informationen über eine Amazon Simple Queue Service-Warteschlange.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSqsQueue` Objekt. Beschreibungen der `AwsSqsQueue` Attribute finden Sie AwsSqsQueueDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSsm` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsSsmPatchCompliance

Das `AwsSsmPatchCompliance` Objekt stellt Informationen über den Status eines Patches auf einer Instanz bereit, basierend auf der Patch-Baseline, die zum Patchen der Instanz verwendet wurde.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSsmPatchCompliance` Objekt. Beschreibungen der `AwsSsmPatchCompliance` Attribute finden Sie AwsSsmPatchComplianceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSsmPatchCompliance": {
```

```
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsStepFunctions` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsStepFunctionStateMachine

Das `AwsStepFunctionStateMachine` Objekt stellt Informationen über eine AWS Step Functions Zustandsmaschine bereit. Dabei handelt es sich um einen Workflow, der aus einer Reihe von ereignisgesteuerten Schritten besteht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsStepFunctionStateMachine` Beschreibungen der `AwsStepFunctionStateMachine` Attribute finden Sie AwsStepFunctionStateMachinein der AWS Security Hub API-Referenz.

Beispiel

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsWaf` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsWafRateBasedRule

Das `AwsWafRateBasedRule` Objekt enthält Details zu einer AWS WAF ratenbasierten Regel für globale Ressourcen. Eine AWS WAF ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Rate-based Zu den Regeln gehört die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRateBasedRule` Objekt. Beschreibungen der `AwsWafRateBasedRule` Attribute finden Sie AwsWafRateBasedRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
```

```
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

Das `AwsWafRegionalRateBasedRule` Objekt enthält Details zu einer ratenbasierten Regel für regionale Ressourcen. Eine ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Rate-based Zu den Regeln gehört die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRateBasedRule` Objekt. Beschreibungen der `AwsWafRegionalRateBasedRule` Attribute finden Sie AwsWafRegionalRateBasedRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

Das `AwsWafRegionalRule` Objekt enthält Details zu einer AWS WAF regionalen Regel. Diese Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRule` Objekt. Beschreibungen der `AwsWafRegionalRule` Attribute finden Sie AwsWafRegionalRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

Das `AwsWafRegionalRuleGroup` Objekt enthält Details zu einer AWS WAF regionalen Regelgruppe. Eine Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRuleGroup` Objekt. Beschreibungen der `AwsWafRegionalRuleGroup` Attribute finden Sie AwsWafRegionalRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
```

```
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`enthält Einzelheiten zu einer AWS WAF regionalen Web-Zugriffskontrollliste (Web Access Control List, Web-ACL). Eine Web-ACL enthält die Regeln, die die Anfragen identifizieren, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRegionalWebAcl` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRegionalWebAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`stellt Informationen zu einer AWS WAF Regel bereit. Eine AWS WAF Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRule` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`stellt Informationen zu einer AWS WAF Regelgruppe bereit. Eine AWS WAF Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRuleGroup` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
```

```
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

Das `AwsWafv2RuleGroup` Objekt enthält Details zu einer AWS WAF V2-Regelgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2RuleGroup` Objekt. Beschreibungen der `AwsWafv2RuleGroup` Attribute finden Sie AwsWafv2RuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
```

```
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

Das `AwsWafWebAcl` Objekt enthält Details zu einer AWS WAF Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafWebAcl` Objekt. Beschreibungen der `AwsWafWebAcl` Attribute finden Sie AwsWafWebAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

Das `AwsWafv2WebAcl` Objekt enthält Details zu einer AWS WAF V2-Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2WebAcl` Objekt. Beschreibungen der `AwsWafv2WebAcl` Attribute finden Sie AwsWafv2WebAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
```

```
}
```

AwsXray Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsXray` Ressourcen.

AWS Security Hub CSPM normalisiert Ergebnisse aus verschiedenen Quellen in ASFF. Hintergrundinformationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

AwsXrayEncryptionConfig

Das `AwsXrayEncryptionConfig` Objekt enthält Informationen über die Verschlüsselungskonfiguration für AWS X-Ray.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsXrayEncryptionConfig` Objekt. Beschreibungen der `AwsXrayEncryptionConfig` Attribute finden Sie AwsXrayEncryptionConfigDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository Objekt in ASFF

Das `CodeRepository` Objekt enthält Informationen über ein externes Code-Repository, das Sie mit AWS Ressourcen verbunden und Amazon Inspector so konfiguriert haben, dass es nach Sicherheitslücken sucht.

Das folgende Beispiel zeigt die ASFF-Syntax (AWS Security Finding Format) für das `CodeRepository` Objekt. Beschreibungen der `CodeRepository` Attribute finden Sie CodeRepositoryDetailsin der AWS Security Hub API-Referenz. Hintergrundinformationen zu ASFF finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Beispiel

```
"CodeRepository": {
```

```
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Behälter Objekt in ASFF

Das folgende Beispiel zeigt die ASFF-Syntax (AWS Security Finding Format) für das `Container` Objekt. Beschreibungen der `Container` Attribute finden Sie ContainerDetailsin der AWS Security Hub API-Referenz. Hintergrundinformationen zu ASFF finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Beispiel

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Sonstige Objekt in ASFF

Im AWS Security Finding Format (ASFF) spezifiziert das `Other` Objekt benutzerdefinierte Felder und Werte. Weitere Informationen zu ASFF finden Sie unter. AWS Format für Sicherheitssuche (ASFF)

Mithilfe des `Other` Objekts können Sie benutzerdefinierte Felder und Werte für eine Ressource angeben. Sie können das `Other` Objekt in den folgenden Fällen verwenden:

- Der Ressourcentyp hat kein entsprechendes `Details` Objekt. Verwenden Sie das `Other` Objekt, um Details für eine Ressource anzugeben.
- Das `Details` Objekt für den Ressourcentyp enthält nicht alle Attribute, die Sie angeben möchten. Verwenden Sie in diesem Fall das `Details` Objekt für den Ressourcentyp, um verfügbare

Attribute anzugeben. Verwenden Sie das `Other` Objekt, um Attribute anzugeben, die sich nicht im typspezifischen `Details` Objekt befinden.

- Der Ressourcentyp gehört nicht zu den angegebenen Typen. Stellen Sie in diesem Fall `Resource.Type` auf ein `Other` und verwenden Sie das `Other` Objekt, um die Details anzugeben.

Typ: Karte mit bis zu 50 Schlüssel-Wert-Paaren

Jedes Schlüssel-Wert-Paar muss die folgenden Anforderungen erfüllen.

- Der Schlüssel muss weniger als 128 Zeichen enthalten.
- Der Wert muss weniger als 1.024 Zeichen enthalten.

Einblicke in Security Hub CSPM anzeigen

In AWS Security Hub CSPM ist ein Einblick eine Sammlung verwandter Ergebnisse. Ein Einblick kann einen bestimmten Sicherheitsbereich identifizieren, der Aufmerksamkeit und Intervention erfordert. Ein Insight könnte beispielsweise auf EC2-Instances hinweisen, die Gegenstand von Ergebnissen sind, die auf schlechte Sicherheitspraktiken hinweisen. Ein Insight bringt Ergebnisse von verschiedenen Ergebnis-Anbietern zusammen.

Jedes Insight wird von einer Gruppe durch Anweisung und optionale Filter definiert. Die Gruppe nach Anweisung gibt an, wie die übereinstimmenden Ergebnisse gruppiert werden sollen, und identifiziert den Elementtyp, für den das Insight gilt. Wenn beispielsweise ein Insight nach Ressourcenbezeichner gruppiert ist, erstellt das Insight eine Liste von Ressourcenbezeichnern. Die optionalen Filter identifizieren die passenden Ergebnisse für den Einblick. Beispielsweise möchten Sie möglicherweise nur Ergebnisse von bestimmten Anbietern oder Ergebnisse sehen, die mit bestimmten Ressourcentypen verknüpft sind.

Security Hub CSPM bietet mehrere integrierte verwaltete Einblicke. Sie können verwaltete Erkenntnisse nicht ändern oder löschen. Um Sicherheitsprobleme nachzuverfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind, können Sie benutzerdefinierte Einblicke erstellen.

Auf der Insights-Seite der AWS Security Hub CSPM-Konsole wird die Liste der verfügbaren Erkenntnisse angezeigt.

Standardmäßig werden in der Liste sowohl verwaltete als auch benutzerdefinierte Erkenntnisse angezeigt. Um die Insight-Liste nach dem Insight-Typ zu filtern, wählen Sie den Insight-Typ aus dem Drop-down-Menü neben dem Filterfeld aus.

- Um alle verfügbaren Erkenntnisse anzuzeigen, wählen Sie Alle Erkenntnisse aus. Dies ist die Standardoption.
- Um nur verwaltete Einblicke anzuzeigen, wählen Sie Security Hub CSPM managed insights.
- Um nur benutzerdefinierte Erkenntnisse anzuzeigen, wählen Sie Benutzerdefinierte Einblicke.

Sie können die Insight-Liste auch nach dem Namen des Insights filtern. Geben Sie dazu in das Filterfeld den Text ein, der zum Filtern der Liste verwendet werden soll. Der Filter unterscheidet nicht zwischen Groß- und Kleinschreibung. Der Filter sucht nach Erkenntnissen, die den Text an einer beliebigen Stelle im Insight-Namen enthalten.

Ein Einblick gibt nur dann Ergebnisse zurück, wenn Sie Integrationen oder Standards aktiviert haben, die zu passenden Ergebnissen führen. Zum Beispiel der verwaltete Einblick 29. Top-Ressourcen nach Anzahl fehlgeschlagener CIS-Prüfungen gibt nur Ergebnisse zurück, wenn Sie eine Version des Benchmark-Standards der Center for Internet Security (CIS) AWS Foundations aktivieren.

Überprüfung und Umsetzung der Erkenntnisse in Security Hub CSPM

Für jeden Einblick bestimmt AWS Security Hub CSPM zunächst die Ergebnisse, die den Filterkriterien entsprechen, und verwendet dann das Gruppierungsattribut, um die übereinstimmenden Ergebnisse zu gruppieren.

Auf der Seite „Einblicke“ in der Konsole können Sie die Ergebnisse und Erkenntnisse einsehen und entsprechende Maßnahmen ergreifen.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthalten die Ergebnisse für verwaltete Einblicke (wenn Sie in der Aggregationsregion angemeldet sind) Ergebnisse aus der Aggregationsregion und verknüpften Regionen. Wenn die Erkenntnisse nicht nach Region gefiltert werden, enthalten die Ergebnisse für benutzerdefinierte Einblicke auch Ergebnisse aus der Aggregationsregion und verknüpften Regionen (wenn Sie in der Aggregationsregion angemeldet sind). In anderen Regionen beziehen sich die Insight-Ergebnisse nur auf diese Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter. the section called “Aggregation von Daten über Regionen hinweg”

Insight-Ergebnisse anzeigen und entsprechende Maßnahmen ergreifen

Die Insight-Ergebnisse bestehen aus einer gruppierten Liste der Ergebnisse für den Insight. Wenn die Erkenntnisse beispielsweise nach Ressourcen-Identifikatoren gruppiert sind, sind die Insight-

Ergebnisse die Liste der Ressourcen-Identifikatoren. Jedes Element in der Ergebnisliste gibt die Anzahl der übereinstimmenden Ergebnisse für dieses Element an.

Wenn die Ergebnisse nach Ressourcen-ID oder Ressourcentyp gruppiert sind, enthalten die Ergebnisse alle Ressourcen, die in den passenden Ergebnissen enthalten sind. Dazu gehören Ressourcen, deren Typ von dem in den Filterkriterien angegebenen Ressourcentyp abweicht. Ein Einblick identifiziert beispielsweise Ergebnisse, die S3-Buckets zugeordnet sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, umfassen die Insight-Ergebnisse beide Ressourcen.

In der Security Hub CSPM-Konsole wird die Ergebnisliste von den meisten bis zu den wenigsten übereinstimmenden Ergebnissen sortiert. Security Hub CSPM kann nur 100 Ergebnisse anzeigen. Wenn es mehr als 100 Gruppierungswerte gibt, werden nur die ersten 100 angezeigt.

Zusätzlich zur Ergebnisliste wird in den Insight-Ergebnissen eine Reihe von Diagrammen angezeigt, die die Anzahl der übereinstimmenden Ergebnisse für die folgenden Attribute zusammenfassen.

- Schweregradbezeichnung — Anzahl der Ergebnisse für jede Schweregradklasse
- AWS-Konto ID — Die fünf wichtigsten Konto-IDs für die übereinstimmenden Ergebnisse
- Ressourcentyp — Die fünf wichtigsten Ressourcentypen für die übereinstimmenden Ergebnisse
- Ressourcen-ID — Die fünf wichtigsten Ressourcen-IDs für die übereinstimmenden Ergebnisse
- Produktname — Die fünf besten Findanbieter für die übereinstimmenden Ergebnisse

Wenn Sie benutzerdefinierte Aktionen konfiguriert haben, können Sie ausgewählte Ergebnisse an eine benutzerdefinierte Aktion senden. Die Aktion muss mit einer CloudWatch Amazon-Regel für den `Security Hub Insight Results` Ereignistyp verknüpft sein. Weitere Informationen finden Sie unter the section called “Automatisierte Reaktion und Problembehebung”. Wenn Sie keine benutzerdefinierten Aktionen konfiguriert haben, ist das Aktionsmenü deaktiviert.

Security Hub CSPM console

Um Insight-Ergebnisse anzuzeigen und entsprechende Maßnahmen zu ergreifen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.

4. Wählen Sie das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.
5. Wählen Sie im Menü Actions (Aktionen) die benutzerdefinierte Aktion aus.

Security Hub CSPM API, AWS CLI

Um Insight-Ergebnisse anzuzeigen und entsprechende Maßnahmen zu ergreifen (API,) AWS CLI

Um Insight-Ergebnisse anzuzeigen, verwenden Sie den >GetInsightResults Betrieb der Security Hub CSPM-API. Wenn Sie die verwenden AWS CLI, führen Sie den get-insight-results Befehl aus.

Um die Erkenntnisse zu identifizieren, für die Ergebnisse zurückgegeben werden sollen, benötigen Sie den Insight-ARN. Verwenden Sie die `GetInsights` API-Operation oder den get-insight-results Befehl, um die Insight-ARNs für benutzerdefinierte Erkenntnisse abzurufen.

Im folgenden Beispiel werden die Ergebnisse für den angegebenen Einblick abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Hinweise zum programmgesteuerten Erstellen benutzerdefinierter Aktionen finden Sie unter. Verwenden benutzerdefinierter Aktionen zum Senden von Ergebnissen und Insight-Ergebnissen an EventBridge

Ergebnisse von Insights anzeigen und entsprechende Maßnahmen ergreifen (Konsole)

In einer Insight-Ergebnisliste auf der Security Hub CSPM-Konsole können Sie die Ergebnisliste für jedes Ergebnis anzeigen.

Um Insight-Ergebnisse anzuzeigen und entsprechende Maßnahmen zu ergreifen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.

4. Um die Liste der Ergebnisse für ein Insight-Ergebnis anzuzeigen, wählen Sie das Element aus der Ergebnisliste aus. Die Ergebnisliste zeigt die aktiven Ergebnisse für das ausgewählte Insight-Ergebnis mit dem Workflow-Status `NEW` oder `NOTIFIED`.

In der Ergebnisliste können Sie die folgenden Aktionen ausführen:

- Ergebnisse im Security Hub CSPM filtern
- Details und Verlauf der Ergebnisse überprüfen
- Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen
- Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden

Verwaltete Einblicke in Security Hub CSPM

AWSSecurity Hub CSPM bietet mehrere verwaltete Einblicke.

Sie können von Security Hub CSPM verwaltete Einblicke nicht bearbeiten oder löschen. Sie können die Insight-Ergebnisse und -Resultate einsehen und Maßnahmen ergreifen. Sie können auch einen verwalteten Insight als Grundlage für einen neuen benutzerdefinierten Insight verwenden.

Wie bei allen Insights gibt ein verwalteter Insight nur Ergebnisse zurück, wenn Sie Produktintegrationen oder Sicherheitsstandards aktiviert haben, die zu passenden Ergebnissen führen können.

Bei Erkenntnissen, die nach Ressourcen-IDs gruppiert sind, enthalten die Ergebnisse die Identifikatoren aller Ressourcen in den entsprechenden Ergebnissen. Dazu gehören Ressourcen, deren Typ sich von dem in den Filterkriterien angegebenen Ressourcentyp unterscheidet. Insight 2 in der folgenden Liste identifiziert beispielsweise Ergebnisse, die mit Amazon S3 S3-Buckets verknüpft sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, umfassen die Insight-Ergebnisse beide Ressourcen.

Security Hub CSPM bietet derzeit die folgenden verwalteten Einblicke:

1. AWSRessourcen mit den meisten Ergebnissen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

2. S3-Buckets mit öffentlichen Lese- oder Schreibberechtigungen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Typ beginnt mit `Effects/Data Exposure`
   - Ressourcentyp ist `AwsS3Bucket`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

3. AMIs, die die meisten Ergebnisse erzeugen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Gruppiert nach: Image-ID der EC2-Instanz

   Filter finden:

   - Ressourcentyp ist `AwsEc2Instance`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

4. EC2-Instances, die mit bekannten Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs) zusammenhängen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Typ beginnt mit `TTPs`
   - Ressourcentyp ist `AwsEc2Instance`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

5. AWSPrincipals mit verdächtiger Zugriffsschlüsselaktivität

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Gruppiert nach: Prinzipalname des IAM-Zugriffsschlüssels

   Filter finden:

   - Ressourcentyp ist `AwsIamAccessKey`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

6. AWSRessourcen und Instanzen, die die Sicherheitsstandards/Best Practices nicht erfüllen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Typ ist `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

7. AWSRessourcen im Zusammenhang mit potenzieller Datenexfiltration

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Der Typ beginnt mit Effects/Data Exfiltration/
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

8. AWSRessourcen, die mit unberechtigtem Ressourcenverbrauch verbunden sind

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

- Typ beginnt mit `Effects/Resource Consumption`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

9. S3-Buckets, die Sicherheitsstandards oder Best Practices nicht erfüllen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Ressourcentyp ist `AwsS3Bucket`
   - Typ ist `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

10. S3-Buckets mit sensiblen Daten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsS3Bucket`
    - Typ beginnt mit `Sensitive Data Identifications/`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

11. Anmeldeinformationen, die möglicherweise in falsche Hände geraten sind

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Sensitive Data Identifications/Passwords/`
    - Datensatzstatus ist `ACTIVE`

- Workflow-Status ist `NEW` oder `NOTIFIED`

12. EC2-Instances mit fehlenden Sicherheits-Patches für wichtige Schwachstellen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Software and Configuration Checks/Vulnerabilities/CVE`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

13. EC2-Instances mit allgemeinem ungewöhnlichem Verhalten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Unusual Behaviors`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

14. EC2-Instances, die über Ports verfügen, auf die aus dem Internet zugegriffen werden kann

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

15. EC2-Instances, die Sicherheitsstandards oder Best Practices nicht erfüllen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWSSecurity Best Practices`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
16. EC2-Instances mit offenem Zugang zum Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
17. EC2-Instances, die mit Ausspähungen durch Widersacher zusammenhängen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit TTPs/Discovery/Recon
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`

- Workflow-Status ist `NEW` oder `NOTIFIED`

18. AWSRessourcen, die mit Malware in Verbindung stehen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Effects/Data Exfiltration/Trojan`
      - `TTPs/Initial Access/Trojan`
      - `TTPs/Command and Control/Backdoor`
      - `TTPs/Command and Control/Trojan`
      - `Software and Configuration Checks/Backdoor`
      - `Unusual Behaviors/VM/Backdoor`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

19. AWSRessourcen im Zusammenhang mit Kryptowährungsproblemen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Effects/Resource Consumption/Cryptocurrency`
      - `TTPs/Command and Control/CryptoCurrency`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

20. AWSRessourcen mit unautorisierten Zugriffsversuchen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

- Typ beginnt mit einer der folgenden Möglichkeiten:
  - `TTPs/Command and Control/UnauthorizedAccess`
  - `TTPs/Initial Access/UnauthorizedAccess`
  - `Effects/Data Exfiltration/UnauthorizedAccess`
  - `Unusual Behaviors/User/UnauthorizedAccess`
  - `Effects/Resource Consumption/UnauthorizedAccess`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

21. Bedrohungsinformationsindikatoren mit den meisten Treffern in der letzten Woche

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Filter finden:

    - Erstellt innerhalb der letzten 7 Tage

22. Top-Konten nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Gruppiert nach: AWS-Konto ID

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

23. Top-Produkte nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Gruppiert nach: Produktname

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

24. Schweregrad nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

Gruppiert nach: Bezeichnung Schweregrad

Filter finden:

- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

25. Top S3-Buckets nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsS3Bucket`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

26. Top-EC2-Instances nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

27. Top-AMIs nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Gruppiert nach: Image-ID der EC2-Instanz

    Filter finden:

    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

28. Top-IAM-Benutzer nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Gruppiert nach: IAM-Zugriffsschlüssel-ID

    Filter finden:

    - Ressourcentyp ist `AwsIamAccessKey`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

29. Top-Ressourcen nach Anzahl fehlgeschlagener CIS-Prüfungen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Generator-ID beginnt mit `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Aktualisiert am letzten Tag
    - Compliance-Status ist `FAILED`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

30. Top-Integrationen nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Gruppiert nach: Produkt ARN

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

31. Ressourcen mit den am meisten fehlgeschlagenen Sicherheitsprüfungen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

    Gruppiert nach: Ressourcen-ID

Filter finden:

- Aktualisiert am letzten Tag
- Compliance-Status ist `FAILED`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

32. IAM-Benutzer mit verdächtigen Aktivitäten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Gruppiert nach: IAM-Benutzer

    Filter finden:

    - Ressourcentyp ist `AwsIamUser`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

33. Ressourcen mit den meisten AWS Health Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - `ProductName`ist gleich `Health`

34. Ressourcen mit den meisten AWS Config Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - `ProductName`ist gleich `Config`

35. Bewerbungen mit den meisten Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Gruppiert nach: ResourceApplicationArn

    Filter finden:

- `RecordState`ist gleich `ACTIVE`
- `Workflow.Status`ist gleich oder `NEW` `NOTIFIED`

Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM

Zusätzlich zu den von AWS Security Hub CSPM verwalteten Erkenntnissen können Sie in Security Hub CSPM benutzerdefinierte Einblicke erstellen, um Probleme zu verfolgen, die für Ihre Umgebung spezifisch sind. Mithilfe benutzerdefinierter Einblicke können Sie eine kuratierte Teilmenge von Problemen verfolgen.

Hier sind einige Beispiele für benutzerdefinierte Einblicke, deren Einrichtung hilfreich sein kann:

- Wenn Sie ein Administratorkonto besitzen, können Sie einen benutzerdefinierten Einblick einrichten, um kritische und schwerwiegende Ergebnisse zu verfolgen, die sich auf Mitgliedskonten auswirken.
- Wenn Sie sich auf einen bestimmten integrierten AWS Dienst verlassen, können Sie einen benutzerdefinierten Einblick einrichten, um die Ergebnisse dieses Dienstes bei kritischen und schwerwiegenden Problemen nachzuverfolgen.
- Wenn Sie sich auf die Integration eines Drittanbieters verlassen, können Sie einen benutzerdefinierten Einblick einrichten, um die Ergebnisse dieses integrierten Produkts bei kritischen und schwerwiegenden Problemen nachzuverfolgen.

Sie können völlig neue benutzerdefinierte Insights erstellen oder von einem vorhandenen benutzerdefinierten oder verwalteten Insight ausgehen.

Jeder Einblick kann mit den folgenden Optionen konfiguriert werden:

- Gruppierungsattribut — Das Gruppierungsattribut bestimmt, welche Elemente in der Insight-Ergebnisliste angezeigt werden. Lautet das Gruppierungsattribut beispielsweise Produktname, zeigen die Insight-Ergebnisse die Anzahl der Ergebnisse an, die jedem Findanbieter zugeordnet sind.
- Optionale Filter — Die Filter grenzen die passenden Ergebnisse für den Insight ein.

  Ein Ergebnis wird nur dann in die Insight-Ergebnisse aufgenommen, wenn es allen bereitgestellten Filtern entspricht. Lauten die Filter beispielsweise „Produktname ist GuardDuty“ und

„Ressourcentyp ist`AwsS3Bucket`“, müssen die passenden Ergebnisse diesen beiden Kriterien entsprechen.

Security Hub CSPM wendet jedoch die boolesche OR-Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Lauten die Filter beispielsweise „Produktname ist“ und GuardDuty „Produktname ist Amazon Inspector“, stimmt ein Ergebnis überein, wenn es entweder von Amazon oder Amazon GuardDuty Inspector generiert wurde.

Wenn Sie die Ressourcen-ID oder den Ressourcentyp als Gruppierungsattribut verwenden, enthalten die Insight-Ergebnisse alle Ressourcen, die in den übereinstimmenden Ergebnissen enthalten sind. Die Liste ist nicht auf Ressourcen beschränkt, die einem Ressourcentypfilter entsprechen. Ein Einblick identifiziert beispielsweise Ergebnisse, die S3-Buckets zugeordnet sind, und gruppiert diese Ergebnisse nach Ressourcen-IDs. Ein passendes Ergebnis enthält sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource. Die Insight-Ergebnisse umfassen beide Ressourcen.

Wenn Sie die regionsübergreifende Aggregation aktivieren und dann einen benutzerdefinierten Einblick erstellen, gilt der Einblick für übereinstimmende Ergebnisse in der Aggregationsregion und verknüpften Regionen. Die Ausnahme ist, wenn Ihr Einblick einen Regionsfilter enthält.

Einen benutzerdefinierten Einblick erstellen

In AWS Security Hub CSPM können benutzerdefinierte Einblicke verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter. Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um einen benutzerdefinierten Einblick in Security Hub CSPM zu erstellen

Security Hub CSPM console

So erstellen Sie einen benutzerdefinierten Einblick (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie Create Insight (Insight erstellen) aus.

4. So wählen Sie das Gruppierungsattribut für den Insight aus:

   a. Wählen Sie das Suchfeld, um die Filteroptionen anzuzeigen.

   b. Wählen Sie Group by (Gruppieren nach).

   c. Wählen Sie das Attribut aus, das verwendet werden soll, um die Ergebnisse zu gruppieren, die mit diesem Einblick verknüpft sind.

   d. Wählen Sie Anwenden aus.

5. Wählen Sie optional weitere Filter aus, die Sie für diesen Einblick verwenden möchten. Definieren Sie für jeden Filter die Filterkriterien und wählen Sie dann Anwenden.

6. Wählen Sie Create Insight (Insight erstellen) aus.

7. Geben Sie einen Insight-Namen ein und wählen Sie dann Create insight aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu erstellen

1. Um einen benutzerdefinierten Einblick zu erstellen, verwenden Sie den CreateInsight Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den create-insight Befehl aus.

2. Füllen Sie den `Name` Parameter mit einem Namen für Ihren benutzerdefinierten Einblick aus.

3. Füllen Sie den `Filters` Parameter aus, um anzugeben, welche Ergebnisse in den Einblick aufgenommen werden sollen.

4. Füllen Sie den `GroupByAttribute` Parameter aus, um anzugeben, welches Attribut verwendet wird, um die in der Erkenntnis enthaltenen Ergebnisse zu gruppieren.

5. Füllen Sie den `SortCriteria` Parameter optional aus, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

Im folgenden Beispiel wird ein benutzerdefinierter Einblick erstellt, der wichtige Ergebnisse mit dem `AwsIamRole` Ressourcentyp enthält. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Um einen benutzerdefinierten Einblick zu erstellen (PowerShell)

1. Verwenden Sie das cmdlet `New-SHUBInsight`.
2. Füllen Sie den `Name` Parameter mit einem Namen für Ihren benutzerdefinierten Einblick.
3. Füllen Sie den `Filter` Parameter aus, um anzugeben, welche Ergebnisse in den Einblick aufgenommen werden sollen.
4. Füllen Sie den `GroupByAttribute` Parameter aus, um anzugeben, welches Attribut verwendet wird, um die in der Erkenntnis enthaltenen Ergebnisse zu gruppieren.

Wenn Sie die regionsübergreifende Aggregation aktiviert haben und dieses Cmdlet aus der Aggregationsregion verwenden, gilt die Erkenntnis für übereinstimmende Ergebnisse aus der Aggregation und den verknüpften Regionen.

Beispiel

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Erstellen eines benutzerdefinierten Einblicks aus einem verwalteten Einblick (nur Konsole)

Sie können keine Änderungen an einem verwalteten Einblick speichern oder löschen. Sie können jedoch einen verwalteten Einblick als Grundlage für einen benutzerdefinierten Einblick verwenden. Diese Option ist nur auf der Security Hub CSPM-Konsole verfügbar.

Um einen benutzerdefinierten Einblick aus einem verwalteten Einblick (Konsole) zu erstellen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie die verwalteten Insights aus, von denen aus Sie arbeiten möchten.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.

   - So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
     a. Um die bestehende Gruppierung zu entfernen, wählen Sie das X neben der Einstellung Gruppieren nach.
     b. Wählen Sie das Suchfeld.
     c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
     d. Wählen Sie Anwenden aus.
   - Um einen Filter aus dem Insight zu entfernen, wählen Sie das eingekreiste X neben dem Filter aus.
   - So fügen Sie dem Insight einen Filter hinzu:
     a. Wählen Sie das Suchfeld.
     b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
     c. Wählen Sie Anwenden aus.
5. Wenn Ihre Aktualisierungen abgeschlossen sind, wählen Sie Create insight (Insight erstellen).
6. Wenn Sie dazu aufgefordert werden, geben Sie einen Insight-Namen ein und wählen Sie dann Create insight aus.

Einen benutzerdefinierten Einblick bearbeiten

Sie können einen vorhandenen benutzerdefinierten Einblick bearbeiten, um den Gruppierungswert und die Filter zu ändern. Nachdem Sie die Änderungen vorgenommen haben, können Sie die Aktualisierungen an den ursprünglichen Insight speichern oder die aktualisierte Version als neuen Insight speichern.

In AWS Security Hub CSPM können benutzerdefinierte Einblicke verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter. Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM

Um einen benutzerdefinierten Einblick zu bearbeiten, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen.

Security Hub CSPM console

Um einen benutzerdefinierten Einblick zu bearbeiten (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie den zu ändernden benutzerdefinierten Insight aus.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.
   - So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
     a. Um die bestehende Gruppierung zu entfernen, wählen Sie das X neben der Einstellung Gruppieren nach.
     b. Wählen Sie das Suchfeld.
     c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
     d. Wählen Sie Anwenden aus.
   - Um einen Filter aus dem Insight zu entfernen, wählen Sie das eingekreiste X neben dem Filter aus.
   - So fügen Sie dem Insight einen Filter hinzu:
     a. Wählen Sie das Suchfeld.
     b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
     c. Wählen Sie Anwenden aus.
5. Wenn Sie die Aktualisierungen abgeschlossen haben, wählen Sie Save insight (Insight speichern).
6. Führen Sie eine der folgenden Aktionen aus, wenn Sie dazu aufgefordert werden:
   - Um den vorhandenen Einblick an Ihre Änderungen anzupassen, wählen Sie Aktualisieren ***<Insight_Name>*** und dann Einblick speichern aus.
   - Um einen neuen Insight mit den Updates zu erstellen, wählen Sie Save new insight (Neuen Insight speichern. Geben Sie einen Insight name (Insight-Namen) an und wählen Sie dann Save insight (Insight speichern) aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu bearbeiten

1. Verwenden Sie den `UpdateInsight` Betrieb der Security Hub CSPM-API. Wenn Sie das verwenden, führen Sie den AWS CLI update-insight Befehl aus.
2. Um den benutzerdefinierten Einblick zu identifizieren, den Sie aktualisieren möchten, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Verwenden Sie die `GetInsights` Operation oder den get-insights Befehl, um den ARN eines benutzerdefinierten Insights abzurufen.
3. Aktualisieren Sie die `GroupByAttribute` Parameter `NameFilters`, und nach Bedarf.

Im folgenden Beispiel wird der angegebene Insight aktualisiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

Um einen benutzerdefinierten Einblick (PowerShell) zu bearbeiten

1. Verwenden Sie das cmdlet `Update-SHUBInsight`.
2. Um den benutzerdefinierten Einblick zu identifizieren, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Verwenden Sie das `Get-SHUBInsight` Cmdlet, um den ARN eines benutzerdefinierten Insights abzurufen.
3. Aktualisieren Sie die `GroupByAttribute` Parameter `NameFilter`, und nach Bedarf.

Beispiel

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
```

```
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Löschen eines benutzerdefinierten Einblicks

In AWS Security Hub CSPM können benutzerdefinierte Einblicke verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter. Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM

Um einen benutzerdefinierten Einblick zu löschen, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen. Sie können einen verwalteten Einblick nicht löschen.

Security Hub CSPM console

Um einen benutzerdefinierten Einblick zu löschen (Konsole)

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Insights aus.
3. Suchen Sie den benutzerdefinierten Insight, der gelöscht werden soll.
4. Um diesen Einblick zu erhalten, wählen Sie das Symbol für weitere Optionen (die drei Punkte in der oberen rechten Ecke der Karte).
5. Wählen Sie Löschen aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu löschen

1. Verwenden Sie den `DeleteInsight` Betrieb der Security Hub CSPM-API. Wenn Sie das verwenden, führen Sie den AWS CLI delete-insight Befehl aus.

2. Um den benutzerdefinierten Einblick zu identifizieren, der gelöscht werden soll, geben Sie den ARN des Einblicks an. Verwenden Sie die `GetInsights` Operation oder den get-insights Befehl, um den ARN eines benutzerdefinierten Einblicks abzurufen.

Im folgenden Beispiel wird der angegebene Insight gelöscht. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

Um einen benutzerdefinierten Einblick () PowerShell zu löschen

1. Verwenden Sie das cmdlet `Remove-SHUBInsight`.
2. Um den benutzerdefinierten Einblick zu identifizieren, geben Sie den ARN des Einblicks an. Verwenden Sie das `Get-SHUBInsight` Cmdlet, um den ARN eines benutzerdefinierten Einblicks abzurufen.

Beispiel

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Ergebnisse in Security Hub CSPM automatisch ändern und darauf reagieren

AWSSecurity Hub CSPM verfügt über Funktionen, die Ergebnisse auf der Grundlage Ihrer Spezifikationen automatisch ändern und entsprechende Maßnahmen ergreifen.

Security Hub CSPM unterstützt derzeit zwei Arten von Automatisierungen:

- Automatisierungsregeln — Automatische Aktualisierung und Unterdrückung von Ergebnissen nahezu in Echtzeit auf der Grundlage von von Ihnen definierter Kriterien.

- Automatisierte Reaktion und Problembehebung — Erstellen Sie benutzerdefinierte EventBridge Amazon-Regeln, die automatische Maßnahmen definieren, die auf der Grundlage bestimmter Ergebnisse und Erkenntnisse ergriffen werden sollen.

Automatisierungsregeln sind hilfreich, wenn Sie Suchfelder im AWS Security Finding Format (ASFF) automatisch aktualisieren möchten. Sie können beispielsweise eine Automatisierungsregel verwenden, um den Schweregrad oder den Workflow-Status von Ergebnissen aus bestimmten Drittanbieter-Integrationen zu aktualisieren. Durch die Verwendung der Automatisierungsregel entfällt die Notwendigkeit, den Schweregrad oder den Workflow-Status jedes Ergebnisses aus diesem Drittanbieterprodukt manuell zu aktualisieren.

EventBridge Regeln sind hilfreich, wenn Sie außerhalb von Security Hub CSPM Maßnahmen in Bezug auf bestimmte Ergebnisse ergreifen oder bestimmte Ergebnisse zur Behebung oder weiteren Untersuchung an Tools von Drittanbietern senden möchten. Die Regeln können verwendet werden, um unterstützte Aktionen auszulösen, z. B. das Aufrufen einer AWS Lambda Funktion oder die Benachrichtigung eines Amazon Simple Notification Service (Amazon SNS) -Themas über ein bestimmtes Ergebnis.

Automatisierungsregeln werden wirksam, bevor EventBridge Regeln angewendet werden. Das heißt, Automatisierungsregeln werden ausgelöst und aktualisieren ein Ergebnis, bevor das Ergebnis EventBridge empfangen wird. EventBridge Die Regeln gelten dann für den aktualisierten Befund.

Bei der Einrichtung von Automatisierungen für Sicherheitskontrollen empfehlen wir, nach der Kontroll-ID und nicht nach Titel oder Beschreibung zu filtern. Security Hub CSPM aktualisiert zwar gelegentlich Titel und Beschreibungen von Steuerelementen, die Kontroll-IDs bleiben jedoch gleich.

Themen

- Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM
- Verwendung EventBridge für automatische Reaktionen und Problembehebungen

Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Sie können Automatisierungsregeln verwenden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Bei der Erfassung der Ergebnisse kann Security Hub CSPM eine Vielzahl von Regelaktionen anwenden, z. B. das Unterdrücken von Ergebnissen, das Ändern ihres Schweregrads und das Hinzufügen von Notizen. Solche Regelaktionen ändern Ergebnisse, die Ihren angegebenen Kriterien entsprechen.

Zu den Anwendungsfällen für Automatisierungsregeln gehören unter anderem die folgenden:

- Erhöhung des Schweregrads eines Ergebnisses auf den Wert, `CRITICAL` wenn sich die Ressourcen-ID des Ergebnisses auf eine geschäftskritische Ressource bezieht.
- Erhöhung des Schweregrads eines Ergebnisses von bis `HIGH` zu, `CRITICAL` wenn das Ergebnis Ressourcen in bestimmten Produktionskonten betrifft.
- Zuweisen bestimmter Ergebnisse, deren Schweregrad einem `INFORMATIONAL` `SUPPRESSED` Workflow-Status entspricht.

Sie können Automatisierungsregeln nur über ein Security Hub CSPM-Administratorkonto erstellen und verwalten.

Die Regeln gelten sowohl für neue als auch für aktualisierte Ergebnisse. Sie können eine benutzerdefinierte Regel von Grund auf neu erstellen oder eine von Security Hub CSPM bereitgestellte Regelvorlage verwenden. Sie können auch mit einer Vorlage beginnen und diese nach Bedarf ändern.

Definition von Regelkriterien und Regelaktionen

Von einem Security Hub CSPM-Administratorkonto aus können Sie eine Automatisierungsregel erstellen, indem Sie ein oder mehrere Regelkriterien und eine oder mehrere Regelaktionen definieren. Wenn ein Ergebnis den definierten Kriterien entspricht, wendet Security Hub CSPM die Regelaktionen darauf an. Weitere Informationen zu verfügbaren Kriterien und Aktionen finden Sie unter. Verfügbare Regelkriterien und Regelaktionen

Security Hub CSPM unterstützt derzeit maximal 100 Automatisierungsregeln für jedes Administratorkonto.

Das Security Hub CSPM-Administratorkonto kann auch Automatisierungsregeln bearbeiten, anzeigen und löschen. Eine Regel gilt für den Abgleich von Ergebnissen im Administratorkonto und all seinen Mitgliedskonten. Durch die Angabe von Mitgliedskonto-IDs als Regelkriterien können Security Hub CSPM-Administratoren auch Automatisierungsregeln verwenden, um Ergebnisse in bestimmten Mitgliedskonten zu aktualisieren oder zu unterdrücken.

Eine Automatisierungsregel gilt nur in dem Land, AWS-Region in dem sie erstellt wurde. Um eine Regel in mehreren Regionen anzuwenden, muss der Administrator die Regel in jeder Region erstellen. Dies kann über die Security Hub CSPM-Konsole, die Security Hub CSPM-API oder erfolgen. AWS CloudFormation Sie können auch ein Bereitstellungsskript für mehrere Regionen verwenden.

Verfügbare Regelkriterien und Regelaktionen

Die folgenden ASFF-Felder (AWSSecurity Finding Format) werden derzeit als Kriterien für Automatisierungsregeln unterstützt:

Regelkriterium	Filteroperatoren	Feldtyp
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge
`ComplianceAssociatedStandardsId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge
`ComplianceSecurityControlId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge
`ComplianceStatus`	`Is, Is Not`	Wählen Sie: `[FAILED,NOT_AVAILABLE ,PASSED,WARNING]`
`Confidence`	`Eq (equal-to), Gte (greater-than-equa`	Zahl

Regelkriterium	Filteroperatoren	Feldtyp
	l), Lte (less-than-equal)	
CreatedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01) T21:47:39.269Z
Criticality	Eq (equal-to), Gte (greater-than-equa l), Lte (less-than-equal)	Zahl
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	Zeichenfolge
FirstObservedAt	Start, End, DateRange	Datum (formatiert als 01.012.2022) T21:47:39.269Z
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	Zeichenfolge
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	Zeichenfolge
LastObservedAt	Start, End, DateRange	Datum (formatiert als 01.012.2022) T21:47:39.269Z
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	Zeichenfolge

Regelkriterium	Filteroperatoren	Feldtyp
NoteUpdatedAt	Start, End, DateRange	Datum (formatiert als 01.012.2022) T21:47:39.269Z
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge

Regelkriterium	Filteroperatoren	Feldtyp
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
ResourceType	Is, Is Not	Wählen Sie (siehe Von ASFF unterstützte Ressourcen)

Regelkriterium	Filteroperatoren	Feldtyp
SeverityLabel	Is, Is Not	Wählen Sie: [CRITICAL,HIGH,, MEDIUMLOW,INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
UpdatedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01) T21:47:39.269Z
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
WorkflowStatus	Is, Is Not	Wählen Sie: [NEW,,,NOTIFIED] RESOLVED SUPPRESSED

Bei Kriterien, die als Zeichenkettenfelder gekennzeichnet sind, wirkt sich die Verwendung verschiedener Filteroperatoren für dasselbe Feld auf die Bewertungslogik aus. Weitere Informationen finden Sie StringFilterin der AWSSecurity Hub CSPM API-Referenz.

Jedes Kriterium unterstützt eine maximale Anzahl von Werten, anhand derer übereinstimmende Ergebnisse gefiltert werden können. Die Grenzwerte für die einzelnen Kriterien finden Sie AutomationRulesFindingFiltersin der AWSSecurity Hub CSPM API-Referenz.

Die folgenden ASFF-Felder werden derzeit als Aktionen für Automatisierungsregeln unterstützt:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Weitere Informationen zu bestimmten ASFF-Feldern finden Sie unter Syntax des AWSSecurity Finding Format (ASFF).

> **Tip**
>
> Wenn Sie möchten, dass Security Hub CSPM keine Ergebnisse für ein bestimmtes Steuerelement generiert, empfehlen wir, das Steuerelement zu deaktivieren, anstatt eine Automatisierungsregel zu verwenden. Wenn Sie eine Kontrolle deaktivieren, beendet Security Hub CSPM die Durchführung von Sicherheitsüberprüfungen und generiert keine Ergebnisse mehr dafür, sodass Ihnen für diese Kontrolle keine Gebühren entstehen. Wir empfehlen die Verwendung von Automatisierungsregeln, um die Werte bestimmter ASFF-Felder für Ergebnisse zu ändern, die definierten Kriterien entsprechen. Weitere Informationen zum Deaktivieren von Steuerelementen finden Sie unter. Deaktivieren der Steuerelemente in Security Hub CSPM

Ergebnisse, die durch Automatisierungsregeln bewertet werden

Eine Automatisierungsregel wertet neue und aktualisierte Ergebnisse aus, die Security Hub CSPM im Rahmen des BatchImportFindingsVorgangs generiert oder aufnimmt, nachdem Sie die Regel erstellt haben. Security Hub CSPM-Updates kontrollieren die Ergebnisse alle 12 bis 24 Stunden oder wenn sich der Status der zugehörigen Ressource ändert. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Automatisierungsregeln bewerten die ursprünglichen Ergebnisse, die vom Anbieter bereitgestellt wurden. Anbieter können mithilfe der Security Hub CSPM-API neue Erkenntnisse bereitstellen und bestehende Ergebnisse aktualisieren. `BatchImportFindings` Wenn die folgenden Felder im ursprünglichen Ergebnis nicht vorhanden sind, füllt Security Hub CSPM die Felder automatisch aus und verwendet dann die ausgefüllten Werte bei der Auswertung durch die Automatisierungsregel:

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

Nachdem Sie eine oder mehrere Automatisierungsregeln erstellt haben, werden die Regeln nicht ausgelöst, wenn Sie Suchfelder mithilfe des Vorgangs aktualisieren. BatchUpdateFindings Wenn Sie eine Automatisierungsregel erstellen und eine `BatchUpdateFindings` Aktualisierung vornehmen, die sich beide auf dasselbe Ergebnisfeld auswirken, legt die letzte Aktualisierung den Wert für dieses Feld fest. Nehmen wir das folgende Beispiel:

1. Sie verwenden die `BatchUpdateFindings` Operation, um den Wert für das `Workflow.Status` Feld eines Ergebnisses von bis `NEW` zu zu ändern`NOTIFIED`.
2. Wenn Sie aufrufen`GetFindings`, hat das `Workflow.Status` Feld jetzt den Wert`NOTIFIED`.
3. Sie erstellen eine Automatisierungsregel, die das `Workflow.Status` Feld des Ergebnisses von `NEW` zu ändert`SUPPRESSED`. (Denken Sie daran, dass Regeln Aktualisierungen ignorieren, die mithilfe des `BatchUpdateFindings` Vorgangs vorgenommen wurden.)
4. Der Suchprovider verwendet den `BatchImportFindings` Vorgang, um den Befund zu aktualisieren, und ändert den Wert für das `Workflow.Status` Feld des Ergebnisses in`NEW`.

5. Wenn Sie aufrufen`GetFindings`, hat das `Workflow.Status` Feld jetzt den Wert`SUPPRESSED`. Dies ist der Fall, weil die Automatisierungsregel angewendet wurde und die Regel die letzte Aktion war, die aufgrund des Ergebnisses ausgeführt wurde.

Wenn Sie eine Regel auf der Security Hub CSPM-Konsole erstellen oder bearbeiten, zeigt die Konsole eine Betaversion von Ergebnissen an, die den Regelkriterien entsprechen. Während Automatisierungsregeln die ursprünglichen Ergebnisse auswerten, die vom Finding-Anbieter gesendet wurden, gibt die Beta-Version der Konsole die Ergebnisse in ihrem endgültigen Zustand wieder, so wie sie als Reaktion auf den GetFindingsVorgang angezeigt würden (d. h. nachdem Regelaktionen oder andere Updates auf das Ergebnis angewendet wurden).

Wie funktioniert die Reihenfolge der Regeln

Beim Erstellen von Automatisierungsregeln weisen Sie jeder Regel eine Reihenfolge zu. Dies bestimmt die Reihenfolge, in der Security Hub CSPM Ihre Automatisierungsregeln anwendet, und ist wichtig, wenn sich mehrere Regeln auf dasselbe Such- oder Findungsfeld beziehen.

Wenn sich mehrere Regelaktionen auf dasselbe Befund- oder Findungsfeld beziehen, gilt die Regel mit dem höchsten numerischen Wert für die Reihenfolge der Regeln zuletzt und hat die endgültige Wirkung.

Wenn Sie eine Regel in der Security Hub CSPM-Konsole erstellen, weist Security Hub CSPM automatisch die Regelreihenfolge auf der Grundlage der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst. Security Hub CSPM wendet nachfolgende Regeln in aufsteigender Reihenfolge an.

Wenn Sie eine Regel über die Security Hub CSPM API oder erstellenAWS CLI, wendet Security Hub CSPM zuerst die Regel mit dem niedrigsten numerischen Wert an. `RuleOrder` Anschließend werden die nachfolgenden Regeln in aufsteigender Reihenfolge angewendet. Wenn mehrere Ergebnisse identisch sind`RuleOrder`, wendet Security Hub CSPM zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die Regel, die zuletzt bearbeitet wurde, gilt zuletzt).

Sie können die Reihenfolge der Regeln jederzeit ändern.

Beispiel für die Reihenfolge der Regeln:

Regel A (Regelreihenfolge ist**1**):

- Kriterien für Regel A

  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` ist `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` ist `NEW`
  - `Workflow.Status` = `ACTIVE`
- Aktionen nach Regel A
  - Update `Confidence` auf `95`
  - Aktualisieren `Severity` auf `CRITICAL`

Regel B (Reihenfolge der Regeln ist**2**):

- Kriterien für Regel B
  - `AwsAccountId` = `123456789012`
- Aktionen nach Regel B
  - Update `Severity` auf `INFORMATIONAL`

Aktionen nach Regel A gelten zuerst für Security Hub CSPM-Ergebnisse, die den Kriterien von Regel A entsprechen. Als Nächstes gelten die Aktionen nach Regel B für Security Hub CSPM-Ergebnisse mit der angegebenen Konto-ID. Da Regel B in diesem Beispiel zuletzt gilt, lautet der Endwert für Ergebnisse aus `Severity` der angegebenen Konto-ID. `INFORMATIONAL` Basierend auf der Regel A-Aktion ist der Endwert von `Confidence` in übereinstimmenden Ergebnissen`95`.

Automatisierungsregeln erstellen

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Sie können eine benutzerdefinierte Automatisierungsregel von Grund auf neu erstellen oder auf der Security Hub CSPM-Konsole eine vorab ausgefüllte Regelvorlage verwenden. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Sie können jeweils nur eine Automatisierungsregel erstellen. Um mehrere Automatisierungsregeln zu erstellen, folgen Sie den Konsolenprozeduren mehrmals oder rufen Sie die API oder den Befehl mehrmals mit den gewünschten Parametern auf.

Sie müssen in jeder Region und jedem Konto, in dem die Regel auf Ergebnisse angewendet werden soll, eine Automatisierungsregel erstellen.

Wenn Sie eine Automatisierungsregel in der Security Hub CSPM-Konsole erstellen, zeigt Ihnen Security Hub CSPM eine Betaversion der Ergebnisse, für die Ihre Regel gilt. Die Betaversion wird derzeit nicht unterstützt, wenn Ihre Regelkriterien einen CONTAINS- oder NOT_CONTAINS-Filter beinhalten. Sie können diese Filter für Zuordnungs- und Zeichenkettenfeldtypen auswählen.

> **Important**
>
> AWSempfiehlt, keine personenbezogenen, vertraulichen oder sensiblen Informationen in den Regelnamen, die Beschreibung oder andere Felder aufzunehmen.

Eine benutzerdefinierte Automatisierungsregel erstellen

Wählen Sie Ihre bevorzugte Methode und führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Automatisierungsregel zu erstellen.

Console

So erstellen Sie eine benutzerdefinierte Automatisierungsregel (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie Regel erstellen aus. Wählen Sie für Regeltyp die Option Benutzerdefinierte Regel erstellen aus.
4. Geben Sie im Abschnitt Regel einen eindeutigen Regelnamen und eine Beschreibung für Ihre Regel ein.
5. Verwenden Sie für Kriterien die Dropdownmenüs Schlüssel, Operator und Wert, um Ihre Regelkriterien anzugeben. Sie müssen mindestens ein Regelkriterium angeben.

   Wenn die von Ihnen ausgewählten Kriterien unterstützt werden, zeigt Ihnen die Konsole eine Betaversion der Ergebnisse, die Ihren Kriterien entsprechen.
6. Verwenden Sie für automatisierte Aktionen die Dropdownmenüs, um anzugeben, welche Ergebnisfelder aktualisiert werden sollen, wenn die Ergebnisse Ihren Regelkriterien entsprechen. Sie müssen mindestens eine Regelaktion angeben.
7. Wählen Sie unter Regelstatus aus, ob die Regel nach ihrer Erstellung aktiviert oder deaktiviert werden soll.

8. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachfolgende Regeln für Ergebnisse ignorieren, die diesen Kriterien entsprechen, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
9. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leichter identifizieren können.
10. Wählen Sie Regel erstellen aus.

API

Um eine benutzerdefinierte Automatisierungsregel (API) zu erstellen

1. Führen Sie die Ausführung `CreateAutomationRule`über das Security Hub CSPM-Administratorkonto aus. Diese API erstellt eine Regel mit einem bestimmten Amazon-Ressourcennamen (ARN).
2. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
3. Legen Sie den `IsTerminal` Parameter auf fest, `true` wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
4. Geben Sie für den `RuleOrder` Parameter die Reihenfolge der Regel an. Security Hub CSPM wendet zuerst Regeln mit einem niedrigeren numerischen Wert für diesen Parameter an.
5. Geben Sie für den `RuleStatus` Parameter an, ob Security Hub CSPM die Regel aktivieren und nach der Erstellung auf Ergebnisse anwenden soll. Der Standardwert ist `ENABLED`, wenn kein Wert angegeben wird. Der Wert von `DISABLED` bedeutet, dass die Regel nach der Erstellung angehalten wird.
6. Geben Sie für den `Criteria` Parameter die Kriterien an, nach denen Security Hub CSPM Ihre Ergebnisse filtern soll. Die Regelaktion gilt für Ergebnisse, die den Kriterien entsprechen. Eine Liste der unterstützten Kriterien finden Sie unterVerfügbare Regelkriterien und Regelaktionen.
7. Geben Sie für den `Actions` Parameter die Aktionen an, die Security Hub CSPM ausführen soll, wenn eine Übereinstimmung zwischen einem Ergebnis und Ihren definierten Kriterien besteht. Eine Liste der unterstützten Aktionen finden Sie unter. Verfügbare Regelkriterien und Regelaktionen

Mit dem folgenden AWS CLI Beispielbefehl wird eine Automatisierungsregel erstellt, die den Workflow-Status und die Notiz der übereinstimmenden Ergebnisse aktualisiert. Dieses Beispiel

ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Eine Automatisierungsregel anhand einer Vorlage erstellen (nur Konsole)

Regelvorlagen spiegeln gängige Anwendungsfälle für Automatisierungsregeln wider. Derzeit unterstützt nur die Security Hub CSPM-Konsole Regelvorlagen. Gehen Sie wie folgt vor, um eine Automatisierungsregel aus einer Vorlage in der Konsole zu erstellen.

Um eine Automatisierungsregel aus einer Vorlage (Konsole) zu erstellen

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Automations aus.

3. Wählen Sie Regel erstellen aus. Wählen Sie als Regeltyp die Option Regel aus Vorlage erstellen aus.
4. Wählen Sie im Dropdownmenü eine Regelvorlage aus.
5. (Optional) Falls für Ihren Anwendungsfall erforderlich, ändern Sie die Abschnitte Regel, Kriterien und Automatisierte Aktion. Sie müssen mindestens ein Regelkriterium und eine Regelaktion angeben.

   Wenn die von Ihnen ausgewählten Kriterien unterstützt werden, zeigt Ihnen die Konsole eine Betaversion der Ergebnisse, die Ihren Kriterien entsprechen.
6. Wählen Sie unter Regelstatus aus, ob die Regel nach ihrer Erstellung aktiviert oder deaktiviert werden soll.
7. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachfolgende Regeln für Ergebnisse ignorieren, die diesen Kriterien entsprechen, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
8. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leichter identifizieren können.
9. Wählen Sie Regel erstellen aus.

Automatisierungsregeln anzeigen

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre vorhandenen Automatisierungsregeln und die Details jeder Regel einzusehen.

Einen Überblick darüber, wie Automatisierungsregeln Ihre Ergebnisse verändert haben, finden Sie unterÜberprüfung der Funddetails und des Verlaufs in Security Hub CSPM.

Console

So zeigen Sie Automatisierungsregeln an (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie einen Regelnamen. Wählen Sie alternativ eine Regel aus.
4. Wählen Sie Aktionen und Ansicht aus.

API

Um Automatisierungsregeln (API) anzuzeigen

1. Um die Automatisierungsregeln für Ihr Konto einzusehen, führen Sie es `ListAutomationRules`vom Security Hub CSPM-Administratorkonto aus. Diese API gibt die Regel-ARNs und andere Metadaten für Ihre Regeln zurück. Für diese API sind keine Eingabeparameter erforderlich, Sie können diese jedoch optional `NextToken` als Paginierungsparameter angeben, `MaxResults` um die Anzahl der Ergebnisse zu begrenzen. Der Anfangswert von `NextToken` sollte sein. `NULL`
2. Weitere Regeldetails, einschließlich der Kriterien und Aktionen für eine Regel, erhalten Sie `BatchGetAutomationRules`über das Security Hub CSPM-Administratorkonto. Geben Sie die ARNs der Automatisierungsregeln an, für die Sie Details benötigen.

   Im folgenden Beispiel werden Details für die angegebenen Automatisierungsregeln abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Automatisierungsregeln bearbeiten

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Nach der Erstellung einer Automatisierungsregel kann der delegierte Security Hub CSPM-Administrator die Regel bearbeiten. Wenn Sie eine Automatisierungsregel bearbeiten, gelten die Änderungen für neue und aktualisierte Ergebnisse, die Security Hub CSPM nach der Regelbearbeitung generiert oder aufnimmt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Inhalt einer Automatisierungsregel zu bearbeiten. Sie können eine oder mehrere Regeln mit einer einzigen Anfrage bearbeiten. Anweisungen zum Bearbeiten der Regelreihenfolge finden Sie unterReihenfolge der Automatisierungsregeln bearbeiten.

Console

So bearbeiten Sie Automatisierungsregeln (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel aus, die Sie bearbeiten möchten. Wählen Sie Aktion und Bearbeiten.
4. Ändern Sie die Regel wie gewünscht und wählen Sie Änderungen speichern.

API

Um Automatisierungsregeln (API) zu bearbeiten

1. Führen Sie die Ausführung `BatchUpdateAutomationRules`über das Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel (n) an, die Sie bearbeiten möchten.
3. Geben Sie die neuen Werte für die Parameter an, die Sie bearbeiten möchten. Sie können jeden Parameter bearbeiten, außer`RuleArn`.

Im folgenden Beispiel für wird die angegebene Automatisierungsregel aktualisiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
```

```
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Reihenfolge der Automatisierungsregeln bearbeiten

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Nach der Erstellung einer Automatisierungsregel kann der delegierte Security Hub CSPM-Administrator die Regel bearbeiten.

Wenn Sie die Regelkriterien und Aktionen unverändert lassen möchten, aber die Reihenfolge ändern möchten, in der Security Hub CSPM eine Automatisierungsregel anwendet, können Sie nur die Reihenfolge der Regeln bearbeiten. Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Reihenfolge der Regeln zu bearbeiten.

Anweisungen zum Bearbeiten der Kriterien oder Aktionen einer Automatisierungsregel finden Sie unterAutomatisierungsregeln bearbeiten.

Console

So bearbeiten Sie die Reihenfolge der Automatisierungsregeln (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel aus, deren Reihenfolge Sie ändern möchten. Wählen Sie Priorität bearbeiten.
4. Wählen Sie Nach oben, um die Priorität der Regel um eine Einheit zu erhöhen. Wählen Sie Nach unten, um die Priorität der Regel um eine Einheit zu verringern. Wählen Sie „Nach oben“, um der Regel die Reihenfolge 1 zuzuweisen (dadurch hat die Regel Vorrang vor anderen bestehenden Regeln).

> **Note**
>
> Wenn Sie eine Regel in der Security Hub CSPM-Konsole erstellen, weist Security Hub CSPM automatisch die Regelreihenfolge auf der Grundlage der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst.

API

Um die Reihenfolge der Automatisierungsregeln (API) zu bearbeiten

1. Verwenden Sie den `BatchUpdateAutomationRules`Vorgang vom Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel (n) an, deren Reihenfolge Sie bearbeiten möchten.
3. Ändern Sie den Wert des `RuleOrder` Felds.

> **Note**
>
> Wenn mehrere Regeln dasselbe haben`RuleOrder`, wendet Security Hub CSPM zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die Regel, die zuletzt bearbeitet wurde, gilt zuletzt).

Automatisierungsregeln löschen oder deaktivieren

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub CSPM automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Wenn Sie eine Automatisierungsregel löschen, entfernt Security Hub CSPM sie aus Ihrem Konto und wendet die Regel nicht mehr auf Ergebnisse an. Als Alternative zum Löschen können Sie eine Regel deaktivieren. Dadurch wird die Regel für die future Verwendung beibehalten, aber Security Hub CSPM wendet die Regel erst auf übereinstimmende Ergebnisse an, wenn Sie sie aktivieren.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen einer Automatisierungsregel. Sie können eine oder mehrere Regeln in einer einzigen Anfrage löschen.

Console

Um Automatisierungsregeln zu löschen oder zu deaktivieren (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel (n) aus, die Sie löschen möchten. Wählen Sie Aktion und Löschen (um eine Regel beizubehalten, sie aber vorübergehend zu deaktivieren, wählen Sie Deaktivieren).
4. Bestätigen Sie Ihre Wahl und wählen Sie Delete (Löschen) aus.

API

Um Automatisierungsregeln (API) zu löschen oder zu deaktivieren

1. Verwenden Sie den `BatchDeleteAutomationRules`Vorgang vom Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den `AutomationRulesArns` Parameter den ARN der Regel (n) an, die Sie löschen möchten (um eine Regel beizubehalten, sie aber vorübergehend zu deaktivieren, geben `DISABLED` Sie den `RuleStatus` Parameter an).

Im folgenden Beispiel für wird die angegebene Automatisierungsregel gelöscht. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Beispiele für Automatisierungsregeln

Dieser Abschnitt enthält Beispiele für Automatisierungsregeln für gängige Security Hub CSPM-Anwendungsfälle. Diese Beispiele entsprechen Regelvorlagen, die auf der Security Hub CSPM-Konsole verfügbar sind.

Erhöhen Sie den Schweregrad auf Kritisch, wenn eine bestimmte Ressource, z. B. ein S3-Bucket, gefährdet ist

In diesem Beispiel werden die Regelkriterien erfüllt, wenn es sich `ResourceId` bei einem Ergebnis um einen bestimmten Amazon Simple Storage Service (Amazon S3) -Bucket handelt. Die Regelaktion besteht darin, den Schweregrad der übereinstimmenden Ergebnisse auf zu ändern`CRITICAL`. Sie können diese Vorlage ändern, um sie auf andere Ressourcen anzuwenden.

Beispiel für eine API-Anfrage:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
```

```
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel für einen CLI-Befehl:

```
$
aws securityhub create-automation-rule \
```

```
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Erhöhen Sie den Schweregrad von Feststellungen, die sich auf Ressourcen in Produktionskonten beziehen

In diesem Beispiel werden die Regelkriterien erfüllt, wenn in bestimmten Produktionskonten ein `HIGH` Schweregrad festgestellt wird. Die Regelaktion besteht darin, den Schweregrad der übereinstimmenden Ergebnisse auf zu ändern`CRITICAL`.

Beispiel für eine API-Anfrage:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
```

```
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel für einen CLI-Befehl:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
```

```
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Informative Ergebnisse unterdrücken

In diesem Beispiel werden die Regelkriterien für die Ergebnisse des `INFORMATIONAL` Schweregrads, die von Amazon an Security Hub CSPM gesendet wurden, abgeglichen. GuardDuty Die Regelaktion besteht darin, den Workflow-Status der übereinstimmenden Ergebnisse auf zu ändern. `SUPPRESSED`

Beispiel für eine API-Anfrage:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
```

```
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel für einen CLI-Befehl:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
```

```
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Verwendung EventBridge für automatische Reaktionen und Problembehebungen

Durch die Erstellung von Regeln in Amazon EventBridge können Sie automatisch auf die Ergebnisse von AWS Security Hub CSPM reagieren. Security Hub CSPM sendet Ergebnisse nahezu in Echtzeit als Ereignisse an EventBridge . Sie können einfache Regeln schreiben, um anzugeben, an welchen Ereignissen Sie interessiert sind und welche automatisierten Maßnahmen ergriffen werden müssen,

wenn ein Ereignis einer Regel entspricht. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Eine AWS Lambda Funktion aufrufen
- Aufrufen des Amazon EC2-Befehls run
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer Zustandsmaschine AWS Step Functions
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange
- Senden eines Funds an ein Ticketing-, Chat-, SIEM- oder Incident-Response- und Management-Tool eines Drittanbieters

Security Hub CSPM sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als EventBridge Ereignisse. Sie können auch benutzerdefinierte Aktionen erstellen, mit denen Sie ausgewählte Ergebnisse und Erkenntnisse an diese Adresse senden können. EventBridge

Anschließend konfigurieren Sie EventBridge Regeln, um auf jeden Ereignistyp zu reagieren.

Weitere Informationen zur Verwendung EventBridge finden Sie im EventBridge Amazon-Benutzerhandbuch .

> **Note**
>
> Als bewährte Methode sollten Sie sicherstellen, dass für die Zugriffsberechtigungen, die Ihren Benutzern gewährt werden, IAM-Richtlinien AWS Identity and Access Management (Least-Privilege-Richtlinien) EventBridge verwendet werden, die nur die erforderlichen Berechtigungen gewähren.
> Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement bei Amazon. EventBridge

Eine Reihe von Vorlagen für kontoübergreifende automatische Antworten und Problembehebungen ist ebenfalls in AWS Solutions verfügbar. Die Vorlagen nutzen EventBridge Eventregeln und Lambda-Funktionen. Sie stellen die Lösung mithilfe von CloudFormation und AWS Systems Manager bereit. Die Lösung kann vollautomatische Reaktions- und Abhilfemaßnahmen erstellen. Sie kann auch benutzerdefinierte Security Hub CSPM-Aktionen verwenden, um vom Benutzer ausgelöste

Reaktions- und Abhilfemaßnahmen zu erstellen. Einzelheiten zur Konfiguration und Verwendung der Lösung finden Sie auf der Lösungsseite von Automated Security Response. AWS

Themen

- Security Hub CSPM-Ereignistypen in EventBridge
- EventBridge Veranstaltungsformate für Security Hub CSPM
- Konfiguration einer EventBridge Regel für Security Hub CSPM-Ergebnisse
- Verwenden benutzerdefinierter Aktionen zum Senden von Ergebnissen und Insight-Ergebnissen an EventBridge

Security Hub CSPM-Ereignistypen in EventBridge

Security Hub CSPM verwendet die folgenden EventBridge Amazon-Ereignistypen zur Integration. EventBridge

Auf dem EventBridge Dashboard für Security Hub CSPM umfasst All Events all diese Ereignistypen.

Alle Ergebnisse (Ergebnisse von Security Hub — Importiert)

Security Hub CSPM sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Security Hub Findings - Imported Ereignisse. Jedes Security Hub Findings - Imported Ereignis enthält ein einzelnes Ergebnis.

Jede `BatchImportFindings` `BatchUpdateFindings` UND-Anfrage löst ein Security Hub Findings - Imported Ereignis aus.

Für Administratorkonten EventBridge enthält der Event-Feed Ereignisse für Ergebnisse sowohl aus ihrem Konto als auch aus ihren Mitgliedskonten.

In einer Aggregationsregion enthält der Event-Feed Ereignisse für Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Cross-Region Die Ergebnisse werden nahezu in Echtzeit in den Event-Feed aufgenommen. Informationen zur Konfiguration der Ergebnisaggregation finden Sie unterthe section called “Aggregation von Daten über Regionen hinweg”.

Sie können Regeln definieren EventBridge , die Ergebnisse automatisch an einen Korrektur-Workflow, ein Drittanbieter-Tool oder ein anderes unterstütztes EventBridge Ziel weiterleiten. Die Regeln können Filter enthalten, die die Regel nur anwenden, wenn das Ergebnis bestimmte Attributwerte enthält.

Sie verwenden diese Methode, um automatisch alle Ergebnisse oder alle Ergebnisse, die bestimmte Merkmale aufweisen, an einen Reaktions- oder Korrektur-Workflow zu senden.

Siehe the section called “Konfiguration einer Regel EventBridge ”.

Ergebnisse für benutzerdefinierte Aktionen (Ergebnisse von Security Hub — Benutzerdefinierte Aktion)

Security Hub CSPM sendet auch Ergebnisse, die mit benutzerdefinierten Aktionen verknüpft sind, EventBridge als Security Hub Findings - Custom Action Ereignisse an.

Dies ist nützlich für Analysten, die mit der Security Hub CSPM-Konsole arbeiten und ein bestimmtes Ergebnis oder eine kleine Gruppe von Ergebnissen an einen Reaktions- oder Behebungsworkflow senden möchten. Sie können eine benutzerdefinierte Aktion für bis zu 20 Funde gleichzeitig auswählen. Jedes Ergebnis wird EventBridge als separates Ereignis an gesendet. EventBridge

Wenn Sie eine benutzerdefinierte Aktion erstellen, weisen Sie ihr eine benutzerdefinierte Aktions-ID zu. Sie können diese ID verwenden, um eine EventBridge Regel zu erstellen, die eine bestimmte Aktion ausführt, nachdem Sie ein Ergebnis erhalten haben, das dieser benutzerdefinierten Aktions-ID zugeordnet ist.

Siehe the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Beispielsweise können Sie in Security Hub CSPM eine benutzerdefinierte Aktion mit dem Namen erstellen. `send_to_ticketing` Anschließend erstellen Sie eine Regel EventBridge, die ausgelöst wird, wenn EventBridge ein Ergebnis eingeht, das die `send_to_ticketing` benutzerdefinierte Aktions-ID enthält. Die Regel beinhaltet eine Logik zum Senden der Funde an Ihr Ticketing-System. Anschließend können Sie die Ergebnisse in Security Hub CSPM auswählen und die benutzerdefinierte Aktion in Security Hub CSPM verwenden, um die Ergebnisse manuell an Ihr Ticketsystem zu senden.

Beispiele dafür, wie Sie Security Hub CSPM-Ergebnisse EventBridge zur weiteren Verarbeitung an Security Hub senden können, finden Sie im Partner Network (APN) -Blog unter So integrieren Sie benutzerdefinierte Aktionen in AWS Security Hub CSPM PagerDuty und So aktivieren Sie benutzerdefinierte Aktionen in AWS Security Hub CSPM. AWS

Insight-Ergebnisse für benutzerdefinierte Aktionen (Ergebnisse von Security Hub Insight)

Sie können auch benutzerdefinierte Aktionen verwenden, um Gruppen von Insight-Ergebnissen EventBridge als Security Hub Insight Results Ereignisse zu senden. Insight-Ergebnisse sind die Ressourcen, die zu einer Erkenntnis passen. Beachten Sie, dass Sie die Ergebnisse nicht an senden

EventBridge, wenn Sie Insight-Ergebnisse an senden EventBridge. Sie senden nur die Ressourcen-IDs, die den Insight-Ergebnissen zugeordnet sind. Sie können bis zu 100 Ressourcenkennungen gleichzeitig senden.

Ähnlich wie bei benutzerdefinierten Aktionen für Ergebnisse erstellen Sie zuerst die benutzerdefinierte Aktion in Security Hub CSPM und dann eine Regel in. EventBridge

Siehe the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Nehmen wir beispielsweise an, Sie sehen ein bestimmtes interessantes Ergebnis, das Sie mit einem Kollegen teilen möchten. In diesem Fall können Sie eine benutzerdefinierte Aktion verwenden, um das Insight-Ergebnis über ein Chat- oder Ticketsystem an den Kollegen zu senden.

EventBridge Veranstaltungsformate für Security Hub CSPM

Die Security Hub Insight Results Ereignistypen Security Hub Findings - Imported Security Findings - Custom Action, und verwenden die folgenden Eventformate.

Das Ereignisformat ist das Format, das verwendet wird, wenn Security Hub CSPM ein Ereignis an sendet. EventBridge

Ergebnisse von Security Hub — Importiert

Security Hub Findings - ImportedEreignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
```

```
        }]
    }
}
```

*<finding content>*ist der Inhalt des Ergebnisses, das durch das Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet ein einzelnes Ergebnis.

Eine vollständige Liste der Suchattribute finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Hinweise zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unterthe section called “Konfiguration einer Regel EventBridge ”.

Ergebnisse von Security Hub — Benutzerdefinierte Aktion

Security Hub Findings - Custom ActionEreignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden. Jedes Ergebnis wird in einem separaten Ereignis gesendet.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*ist der Inhalt des Ergebnisses, das vom Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet ein einzelnes Ergebnis.

Eine vollständige Liste der Suchattribute finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Hinweise zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unterthe section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Ergebnisse von Security Hub Insight

Security Hub Insight ResultsEreignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Informationen zum Erstellen einer EventBridge Regel, die durch diese Ereignisse ausgelöst wird, finden Sie unter. the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”

Konfiguration einer EventBridge Regel für Security Hub CSPM-Ergebnisse

Sie können in Amazon eine Regel erstellen EventBridge , die eine Aktion definiert, die ausgeführt werden soll, wenn ein Security Hub Findings - Imported Ereignis eingeht. Security Hub Findings

- ImportedEreignisse werden durch Aktualisierungen der `BatchUpdateFindings` Operationen `BatchImportFindings` und ausgelöst.

Jede Regel enthält ein Ereignismuster, das die Ereignisse identifiziert, die die Regel auslösen. Das Ereignismuster enthält immer die Ereignisquelle (`aws.securityhub`) und den Ereignistyp (Security Hub Findings — Imported). Das Ereignismuster kann auch Filter angeben, um die Ergebnisse zu identifizieren, für die die Regel gilt.

Die Ereignisregel identifiziert dann die Regelziele. Bei den Zielen handelt es sich um die Aktionen, die ergriffen werden EventBridge müssen, wenn ein Ereignis von Security Hub Findings — Imported eingeht und das Ergebnis den Filtern entspricht.

Die hier bereitgestellten Anweisungen verwenden die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben in Amazon EventBridge Logs ermöglicht. CloudWatch

Sie können auch den `PutRule` Betrieb der API verwenden. EventBridge Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Informationen zur erforderlichen Richtlinie finden Sie unter CloudWatch Logs-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

Format des Ereignismusters

Das Format des Ereignismusters für Security Hub Findings — Importierte Ereignisse lautet wie folgt:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifiziert Security Hub CSPM als den Dienst, der das Ereignis generiert.
- `detail-type`identifiziert den Ereignistyp.

- `detail`ist optional und stellt die Filterwerte für das Ereignismuster bereit. Wenn das Ereignismuster kein `detail` Feld enthält, lösen alle Ergebnisse die Regel aus.

Sie können die Ergebnisse anhand eines beliebigen Ergebnisattributs filtern. Für jedes Attribut geben Sie ein kommagetrenntes Array mit einem oder mehreren Werten an.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Wenn Sie mehr als einen Wert für ein Attribut angeben, werden diese Werte durch verknüpft. `OR` Ein Ergebnis entspricht dem Filter für ein einzelnes Attribut, wenn das Ergebnis einen der aufgelisteten Werte enthält. Wenn Sie beispielsweise `INFORMATIONAL` sowohl `LOW` als auch Werte für angeben`Severity.Label`, stimmt das Ergebnis überein, wenn es den Schweregrad entweder `INFORMATIONAL` oder hat`LOW`.

Die Attribute werden durch verknüpft`AND`. Ein Ergebnis stimmt überein, wenn es den Filterkriterien für alle angegebenen Attribute entspricht.

Wenn Sie einen Attributwert angeben, muss dieser die Position dieses Attributs innerhalb der ASFF-Struktur (AWS Security Finding Format) widerspiegeln.

> **Tip**
>
> Beim Filtern von Kontrollergebnissen empfehlen wir, die Felder `SecurityControlId` oder `SecurityControlArn` ASFF als Filter zu verwenden und nicht die Felder oder oder. `Title` `Description` Die letztgenannten Felder können sich gelegentlich ändern, wohingegen die Kontroll-ID und der ARN statische Identifikatoren sind.

Im folgenden Beispiel enthält das Ereignismuster Filterwerte für `ProductArn` und. Ein Ergebnis stimmt also überein`Severity.Label`, wenn es von Amazon Inspector generiert wurde und den Schweregrad entweder `INFORMATIONAL` oder `LOW` hat.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
```

```
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Eine Ereignisregel erstellen

Sie können ein vordefiniertes Ereignismuster oder ein benutzerdefiniertes Ereignismuster verwenden, um eine Regel in zu erstellen EventBridge. Wenn Sie ein vordefiniertes Muster auswählen, füllt es EventBridge automatisch `source` und aus`detail-type`. EventBridge enthält auch Felder zur Angabe von Filterwerten für die folgenden Suchattribute:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Um eine EventBridge Regel zu erstellen (Konsole)

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Erstellen Sie mithilfe der folgenden Werte eine EventBridge Regel, die das Auffinden von Ereignissen überwacht:
   - Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
   - Wählen Sie aus, wie das Ereignismuster erstellt werden soll.

Um das Event-Muster zu erstellen mit...	Vorgehensweise	
Eine Vorlage	Wählen Sie im Abschnitt Event-Muster die folgenden Optionen aus: • Als Event source (Ereignisquelle) wählen Sie AWS -Services aus. • Wählen Sie für AWS Service Security Hub aus. • Wählen Sie als Ereignistyp die Option Security Hub Findings — Imported aus. • (Optional) Fügen Sie Filterwerte hinzu, um die Regel spezifischer zu gestalten. Um die Regel beispielsweise auf Ergebnisse mit aktivem Datensatzstatus zu beschränken, wählen Sie für Bestimmte Datensatzstatus (e) die Option Aktiv aus.	

Um das Event-Muster zu erstellen mit...	Vorgehensweise	
Ein benutzerdefiniertes Ereignismuster (Verwenden Sie ein benutzerdefiniertes Muster, wenn Sie Ergebnisse anhand von Attributen filtern möchten, die nicht in der EventBridge Konsole angezeigt werden.)	• Wählen Sie im Abschnitt Ereignismuster die Option Benutzerdefinierte Muster (JSON-Editor) aus, und fügen Sie dann das folgende Ereignismuster in den Textbereich ein: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }` • Aktualisieren Sie das Ereignismuster, sodass es das Attribut und die Attributwerte enthält, die Sie als Filter verwenden möchten. Verwenden Sie beispielsweise das folgende	

Um das Event-Muster zu erstellen mit...	Vorgehensweise	
	Musterbeispiel, um die Regel auf Ergebnisse anzuwendenTRUE_POSITIVE , die den Überprüfungsstatus von haben: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Wählen Sie für Zieltypen die Option AWS Service aus, und wählen Sie für Wählen Sie ein Ziel aus, z. B. ein Amazon SNS-Thema oder eine AWS Lambda Funktion. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.

Einzelheiten zum Erstellen von Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren.

Verwenden benutzerdefinierter Aktionen zum Senden von Ergebnissen und Insight-Ergebnissen an EventBridge

Um benutzerdefinierte AWS Security Hub CSPM-Aktionen zum Senden von Ergebnissen oder Erkenntnissen an Amazon zu verwenden EventBridge, erstellen Sie zunächst die benutzerdefinierte Aktion in Security Hub CSPM. Anschließend können Sie Regeln definieren, die für Ihre EventBridge benutzerdefinierten Aktionen gelten.

Sie können bis zu 50 benutzerdefinierte Aktionen erstellen.

Wenn Sie die regionsübergreifende Aggregation aktivieren und Ergebnisse aus der Aggregationsregion verwalten, erstellen Sie benutzerdefinierte Aktionen in der Aggregationsregion.

Die Regel in EventBridge verwendet den Amazon-Ressourcennamen (ARN) aus der benutzerdefinierten Aktion.

Eine benutzerdefinierte Aktion erstellen

Wenn Sie eine benutzerdefinierte Aktion in AWS Security Hub CSPM erstellen, geben Sie ihren Namen, eine Beschreibung und eine eindeutige Kennung an.

Eine benutzerdefinierte Aktion gibt an, welche Aktionen ausgeführt werden sollen, wenn ein EventBridge Ereignis einer EventBridge Regel entspricht. Security Hub CSPM sendet jedes Ergebnis EventBridge als Ereignis an.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine benutzerdefinierte Aktion zu erstellen.

Console

Um eine benutzerdefinierte Aktion in Security Hub CSPM (Konsole) zu erstellen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Custom actions (Benutzerdefinierte Aktionen) aus.
3. Wählen Sie Create custom action (Benutzerdefinierte Aktion erstellen) aus.
4. Machen Sie für die Aktion Angaben bei Name, Description (Beschreibung) und Custom action ID (Benutzerdefinierte Aktions-ID).

Der Name muss weniger als 20 Zeichen lang sein.

Die benutzerdefinierte Aktions-ID muss für jedes AWS Konto eindeutig sein.

5. Wählen Sie Create custom action (Benutzerdefinierte Aktion erstellen) aus.
6. Notieren Sie sich den Custom action ARN (Benutzerdefinierter Aktions-ARN). Sie müssen den ARN verwenden, wenn Sie eine Regel erstellen, um sie in EventBridge dieser Aktion zuzuordnen.

API

Um eine benutzerdefinierte Aktion (API) zu erstellen

Verwenden Sie die CreateActionTarget Operation. Wenn Sie den verwenden AWS CLI, führen Sie den Befehl https://docs.aws.amazon.com/cli/latest/reference/securityhub/create-action-target.html create-action-target aus.

Im folgenden Beispiel wird eine benutzerdefinierte Aktion erstellt, um Ergebnisse an ein Problembehebungstool zu senden. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definieren einer Regel in EventBridge

Um eine benutzerdefinierte Aktion in Amazon auszulösen EventBridge, müssen Sie eine entsprechende Regel in erstellen. EventBridge Die Regeldefinition beinhaltet den Amazon-Ressourcennamen (ARN) der benutzerdefinierten Aktion.

Das Ereignismuster für das Ereignis Security Hub Findings — Custom Action hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
```

```
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Das Ereignismuster für ein Security Hub Insight Results-Ereignis hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

In beiden Mustern *<custom action ARN>* ist dies der ARN einer benutzerdefinierten Aktion. Sie können eine Regel konfigurieren, die für mehr als eine benutzerdefinierte Aktion gilt.

Die hier bereitgestellten Anweisungen beziehen sich auf die EventBridge Konsole. Wenn Sie die Konsole verwenden, erstellt EventBridge automatisch die erforderliche ressourcenbasierte Richtlinie, die das Schreiben in Logs EventBridge ermöglicht. CloudWatch

Sie können auch den `PutRule` API-Betrieb der API verwenden. EventBridge Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Einzelheiten zur erforderlichen Richtlinie finden Sie unter CloudWatch Logs-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

Um eine Regel in EventBridge (EventBridge Konsole) zu definieren

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
5. Wählen Sie für Event Bus den Event Bus aus, den Sie dieser Regel zuordnen möchten. Wenn Sie möchten, dass diese Regel mit Ereignissen aus Ihrem eigenen Konto übereinstimmt, wählen Sie Standard aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird es stets an den Standard-Event-Bus Ihres Kontos weitergeleitet.

6. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie für den AWS Service Security Hub.
12. Führen Sie für Type (Typ) eine der folgenden Aktionen aus:

    - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Findings — Custom Action.
    - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Insight-Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Insight-Ergebnisse.
13. Wählen Sie Spezifische benutzerdefinierte Aktions-ARNs und fügen Sie eine benutzerdefinierte Aktions-ARN hinzu.

    Wenn die Regel für mehrere benutzerdefinierte Aktionen gilt, wählen Sie Hinzufügen, um weitere ARNs für benutzerdefinierte Aktionen hinzuzufügen.
14. Wählen Sie Weiter aus.
15. Wählen Sie unter Ziele auswählen das Ziel aus und konfigurieren Sie es, das aufgerufen werden soll, wenn diese Regel erfüllt wird.
16. Wählen Sie Weiter aus.
17. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
18. Wählen Sie Weiter aus.
19. Überprüfen Sie die Details der Regel und wählen Sie dann Regel erstellen aus.

    Wenn Sie eine benutzerdefinierte Aktion für Ergebnisse oder Insight-Ergebnisse in Ihrem Konto ausführen, werden Ereignisse in generiert EventBridge.

Auswahl einer benutzerdefinierten Aktion für Ergebnisse und Erkenntnisergebnisse

Nachdem Sie benutzerdefinierte AWS Security Hub CSPM-Aktionen und EventBridge Amazon-Regeln erstellt haben, können Sie Ergebnisse und Erkenntnisse EventBridge zur automatischen Verwaltung und Verarbeitung an diese Adresse senden.

Ereignisse werden EventBridge nur an das Konto gesendet, in dem sie angezeigt werden. Wenn Sie ein Ergebnis mit einem Administratorkonto anzeigen, wird das Ereignis EventBridge an das Administratorkonto gesendet.

Damit AWS API-Aufrufe wirksam sind, müssen die Implementierungen des Zielcodes die Rollen auf Mitgliedskonten umstellen. Das bedeutet auch, dass die Rolle, in die Sie wechseln, jedem Mitglied zugewiesen werden muss, wenn Maßnahmen erforderlich sind.

Um Ergebnisse an EventBridge (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Zeigt eine Liste der Ergebnisse an:
   - Unter Ergebnisse können Sie die Ergebnisse aller aktivierten Produktintegrationen und Steuerelemente einsehen.
   - Unter Sicherheitsstandards können Sie zu einer Liste der Ergebnisse navigieren, die aus einer bestimmten Kontrolle generiert wurden. Weitere Informationen finden Sie unter Überprüfung der Details der Kontrollen in Security Hub CSPM.
   - Unter Integrationen können Sie zu einer Liste der Ergebnisse navigieren, die von einer aktivierten Integration generiert wurden. Weitere Informationen finden Sie unter Ergebnisse einer Security Hub CSPM-Integration anzeigen.
   - In Insights können Sie zu einer Ergebnisliste für ein Insight-Ergebnis navigieren. Weitere Informationen finden Sie unter Überprüfung und Umsetzung der Erkenntnisse in Security Hub CSPM.
3. Wählen Sie die Ergebnisse aus, an die Sie senden möchten EventBridge. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.
4. Wählen Sie unter Aktionen die benutzerdefinierte Aktion aus, die der anzuwendenden EventBridge Regel entspricht.

   Security Hub CSPM sendet für jedes Ergebnis ein separates Ereignis „Security Hub Findings — Custom Action“.

Um Insight-Ergebnisse an EventBridge (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/

2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie auf der Seite Insights den Insight aus, der die Ergebnisse enthält, an die gesendet werden soll. EventBridge
4. Wählen Sie die Insight-Ergebnisse aus, an die gesendet werden soll EventBridge. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.
5. Wählen Sie unter Aktionen die benutzerdefinierte Aktion aus, die der anzuwendenden EventBridge Regel entspricht.

Arbeiten mit dem Dashboard in Security Hub CSPM

Auf der Security Hub CSPM-Konsole zeigt das Übersichts-Dashboard eine Zusammenfassung Ihrer Risiken, Angriffssequenzen und Sicherheitsvorkehrungen. Dieses Dashboard hilft Ihnen dabei, Risiken und Angriffssequenzen auf der Grundlage des Schweregrads und der Kontoabdeckung für verschiedene Sicherheitsfunktionen zu identifizieren. Jedes Mal, wenn Sie das Dashboard öffnen, wird es automatisch aktualisiert. Beachten Sie jedoch, dass Sicherheitsbewertungen und Kontrollstatus alle 24 Stunden aktualisiert werden.

Sie können das Übersichts-Dashboard anpassen, indem Sie verschiedene Sicherheits-Widgets hinzufügen oder daraus entfernen. Sie können auch Filterkriterien angeben, um bestimmte Datentypen abzurufen und anzuzeigen. Wenn Sie das Dashboard anpassen, speichert Security Hub Ihre Anpassungseinstellungen. Wenn andere Benutzer Ihres Kontos das Dashboard anpassen, werden ihre Änderungen unabhängig von Ihren Anpassungseinstellungen gespeichert.

Wenn Sie die regionsübergreifende Aggregation in Security Hub CSPM konfiguriert haben, zeigt das Übersichts-Dashboard Ihre aggregierten Daten an. Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto für eine Organisation handelt, umfassen die Daten Ergebnisse für Ihr Konto und Ihre Mitgliedskonten. Wenn es sich bei Ihrem Konto um ein Mitgliedskonto oder ein eigenständiges Konto handelt, enthalten die Daten nur Ergebnisse für Ihr Konto.

Themen

- Verfügbare Widgets für das Übersichts-Dashboard
- Filtern des Übersichts-Dashboards in Security Hub CSPM
- Anpassen des Übersichts-Dashboards in Security Hub CSPM

Verfügbare Widgets für das Übersichts-Dashboard

Das Übersichts-Dashboard enthält Widgets, die die aktuelle Bedrohungslandschaft der Cloud-Sicherheit widerspiegeln und sich dabei an den Sicherheitsabläufen und Erfahrungen der AWS Kunden orientieren. Einige Widgets werden standardmäßig angezeigt, andere nicht. Sie können Ihre Ansicht des Dashboards anpassen, indem Sie Widgets hinzufügen oder entfernen.

Um ein Widget hinzuzufügen, wählen Sie oben im Dashboard die Option Widget hinzufügen aus. Sie können dann die Liste der verfügbaren Widgets durchsuchen oder den Titel eines Widgets in die Suchleiste eingeben. Wenn Sie das hinzuzufügende Widget gefunden haben, ziehen Sie es an die Stelle, an der es auf dem Dashboard angezeigt werden soll. Weitere Informationen finden Sie unter Das Dashboard anpassen.

Standardmäßig werden Widgets angezeigt

Standardmäßig enthält das Übersichts-Dashboard die folgenden Widgets.

Sequenzen der wichtigsten Bedrohungen

Zeigt die Bedrohungssequenzen mit dem höchsten Schweregrad an. Die Ergebnisse der Bedrohungssequenz, bei Amazon als Ergebnisse der Angriffssequenz bekannt GuardDuty, korrelieren mehrere Ereignisse, um potenzielle Bedrohungen für Ihre AWS Umgebung zu identifizieren. Zu den Bedrohungssequenzen können aktuelle oder kürzlich aufgetretene Angriffe (innerhalb eines 24-Stunden-Zeitfensters) in Ihrer Umgebung gehören, die wiederum zu weiteren Bedrohungen führen können. Sie müssen GuardDuty S3-Schutz aktiviert haben GuardDuty , um Ergebnisse der Bedrohungssequenz in Security Hub CSPM empfangen zu können.

Die größten Risiken

Zeigt eine Zusammenfassung der wichtigsten Risiken in Ihrer Umgebung an. Im oberen Bereich des Widgets wird die Anzahl der Risiken für jeden Schweregrad angezeigt. Sie können einen Schweregrad auswählen, um zur Seite Risiken zu gelangen, auf der die Risiken nach dem ausgewählten Schweregrad gefiltert werden. Die Risiken, die in Ihrer Umgebung am häufigsten vorkommen, werden zuerst angezeigt. Dieses Widget hilft Ihnen bei der Priorisierung der Risiken, die gemindert werden müssen.

Sicherheitsabdeckung

Fasst den Umfang Ihres Sicherheitsschutzes auf der Grundlage der Ergebnisse der Deckungskontrolle zusammen. Bei der Deckungskontrolle wird geprüft, ob ein bestimmtes Objekt AWS-Service und seine Funktionen aktiviert sind (z. B.[Macie.1] Amazon Macie sollte aktiviert

sein). Mit diesem Widget können Sie sicherstellen, dass Sie über PASSED Ergebnisse für die Deckungskontrolle verfügen. Die Security Hub CSPM-Konsole bietet Links aus diesem Widget, mit denen Sie fehlende Sicherheitsfunktionen aktivieren können. Wir empfehlen, die zentrale Konfiguration zu verwenden, um fehlende Sicherheitsfunktionen für mehrere AWS-Konten und zu aktivieren. AWS-Regionen Weitere Informationen finden Sie unter Grundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Sicherheitsstandards

Zeigt Ihre aktuelle zusammenfassende Sicherheitsbewertung und die Sicherheitsbewertung für jeden Security Hub CSPM-Standard an. Sicherheitswerte, die zwischen 0 und 100 Prozent liegen, stellen den Anteil der bestandenen Kontrollen im Verhältnis zu all Ihren aktivierten Kontrollen dar. Weitere Informationen zu diesen Bewertungen finden Sie unter. Methode zur Berechnung der Sicherheitswerte Dieses Widget hilft Ihnen dabei, Ihren allgemeinen Sicherheitsstatus zu verstehen.

Anlagen mit den meisten Ergebnissen

Bietet einen Überblick über die Ressourcen, Konten und Anwendungen mit den meisten Ergebnissen. Die Liste ist in absteigender Reihenfolge nach der Anzahl der Ergebnisse sortiert. Im Widget zeigt jede Registerkarte die sechs wichtigsten Elemente in dieser Kategorie, gruppiert nach Schweregrad und Ressourcentyp. Wenn Sie in der Spalte Ergebnisse insgesamt eine Zahl auswählen, öffnet Security Hub CSPM eine Seite, auf der die Ergebnisse für das Asset angezeigt werden. Mit diesem Widget können Sie schnell erkennen, welche Ihrer Kernressourcen potenzielle Sicherheitsbedrohungen bergen.

Ergebnisse nach Regionen

Zeigt die Gesamtzahl der Ergebnisse, gruppiert nach Schweregrad, in jedem Fall an, AWS-Region in dem Security Hub CSPM aktiviert ist. Dieses Widget hilft Ihnen dabei, Sicherheitsprobleme zu identifizieren, die möglicherweise bestimmte Regionen betreffen. Wenn Sie das Dashboard in Ihrer Aggregationsregion öffnen, hilft Ihnen dieses Widget dabei, potenzielle Sicherheitsprobleme in jeder verknüpften Region zu überwachen.

Die häufigsten Bedrohungsarten

Bietet eine Aufschlüsselung der 10 häufigsten Bedrohungstypen in Ihrer AWS Umgebung. Dazu gehören Bedrohungen wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen.

Um diese Daten anzeigen zu können, GuardDuty muss Amazon aktiviert sein. Wenn ja, wählen Sie in diesem Widget einen Bedrohungstyp aus, um die GuardDuty Konsole zu öffnen und die

Ergebnisse zu dieser Bedrohung zu überprüfen. Dieses Widget hilft Ihnen dabei, potenzielle Bedrohungen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Sicherheitslücken in Software durch Exploits

Bietet eine Zusammenfassung der Softwareschwachstellen, die in Ihrer AWS Umgebung bestehen und für die bereits bekannte Exploits vorliegen. Sie können sich auch eine Aufschlüsselung der Sicherheitslücken ansehen, für die es Lösungen gibt und für die es keine gibt.

Um diese Daten anzeigen zu können, muss Amazon Inspector aktiviert sein. Wenn ja, wählen Sie eine Statistik in diesem Widget aus, um die Amazon Inspector Inspector-Konsole zu öffnen und weitere Details zu der Sicherheitslücke zu überprüfen. Dieses Widget hilft Ihnen dabei, Softwareschwachstellen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Neue Erkenntnisse im Laufe der Zeit

Zeigt Trends bei der Anzahl neuer täglicher Ergebnisse in den letzten 90 Tagen. Sie können die Daten nach Schweregrad oder nach Anbieter aufschlüsseln, um zusätzlichen Kontext zu erhalten. Mithilfe dieses Widgets können Sie nachvollziehen, ob das gefundene Volumen in den letzten 90 Tagen zu bestimmten Zeiten angestiegen oder gesunken ist.

Ressourcen mit den meisten Ergebnissen

Bietet eine Zusammenfassung der Ressourcen, die zu den meisten Ergebnissen geführt haben, aufgeschlüsselt nach den folgenden Ressourcentypen: Amazon Simple Storage Service (Amazon S3) -Buckets, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Lambda Funktionen.

Im Widget konzentriert sich jede Registerkarte auf einen der vorherigen Ressourcentypen und listet die 10 Ressourcen-Instances auf, die die meisten Ergebnisse generiert haben. Um die Ergebnisse für eine bestimmte Ressource zu überprüfen, wählen Sie die Ressourceninstanz aus. Dieses Widget hilft Ihnen bei der Suche nach Sicherheitsergebnissen, die mit gängigen AWS Ressourcen verknüpft sind.

Widgets sind standardmäßig ausgeblendet

Die folgenden Widgets sind auch für das Übersichts-Dashboard verfügbar, sie sind jedoch standardmäßig ausgeblendet.

AMIs mit den meisten Ergebnissen

Stellt eine Liste der 10 Amazon Machine Images (AMIs) bereit, die die meisten Ergebnisse generiert haben. Diese Daten sind nur verfügbar, wenn Amazon EC2 für Ihr Konto aktiviert ist. Auf diese Weise können Sie ermitteln, welche AMIs potenzielle Sicherheitsrisiken darstellen.

IAM-Prinzipale mit den meisten Ergebnissen

Stellt eine Liste der 10 AWS Identity and Access Management (IAM) -Benutzer bereit, die die meisten Ergebnisse generiert haben. Dieses Widget hilft Ihnen bei der Ausführung von Verwaltungs- und Abrechnungsaufgaben. Es zeigt Ihnen, welche Benutzer am meisten zur Nutzung von Security Hub CSPM beitragen.

Konten mit den meisten Ergebnissen (nach Schweregrad)

Zeigt eine grafische Darstellung der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Schweregrad. Mithilfe dieses Widgets können Sie bestimmen, auf welche Konten Sie sich bei der Analyse und Problembehebung konzentrieren sollten.

Konten mit den meisten Ergebnissen (nach Ressourcentyp)

Zeigt ein Diagramm der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Ressourcentyp. Mit diesem Widget können Sie bestimmen, welche Konten und Ressourcentypen für die Analyse und Problembehebung priorisiert werden müssen.

Einblicke

Führt fünf von Security Hub CSPM verwaltete Erkenntnisse und die Anzahl der Ergebnisse auf, die sie generiert haben. Insights identifizieren einen bestimmten Sicherheitsbereich, der Aufmerksamkeit erfordert.

Aktuelle Erkenntnisse aus AWS Integrationen

Zeigt die Anzahl der Ergebnisse an, die Sie in Security Hub CSPM von integrated erhalten haben. AWS-Services Außerdem wird angezeigt, wann Sie zuletzt Ergebnisse von den einzelnen integrierten Diensten erhalten haben. Dieses Widget bietet konsolidierte Ergebnisdaten aus mehreren AWS-Services. Wählen Sie einen integrierten Service aus, um weitere Informationen zu erhalten. Security Hub CSPM öffnet dann die Konsole für diesen Dienst.

Filtern des Übersichts-Dashboards in Security Hub CSPM

Sie können das Übersichts-Dashboard auf der Security Hub CSPM-Konsole so kuratieren, dass es nur die Sicherheitsdaten enthält, die für Sie am relevantesten sind. Wenn Sie beispielsweise Mitglied

eines Anwendungsteams sind, können Sie eine spezielle Ansicht für eine kritische Anwendung in Ihrer Produktionsumgebung erstellen. Wenn Sie Mitglied eines Sicherheitsteams sind, können Sie eine spezielle Ansicht erstellen, die Ihnen hilft, sich auf Ergebnisse mit hohem Schweregrad zu konzentrieren.

Um diese kuratierten Ansichten zu erstellen, geben Sie Filterkriterien in das Filterfeld über dem Dashboard ein. Wenn Sie Filterkriterien anwenden, gelten die Kriterien für alle Daten und Widgets im Dashboard, mit Ausnahme der Daten in den Widgets „Einblicke“ und „Sicherheitsstandards“. Eine Liste der verfügbaren Widgets auf dem Dashboard finden Sie unterVerfügbare Widgets für das Übersichts-Dashboard.

Sie können die Daten mithilfe der folgenden Felder filtern:

- Account name (Kontoname)
- Konto-ID
- Anwendungs-ARN
- Anwendungsname
- Produktname (für ein Produkt AWS-Service oder ein Produkt eines Drittanbieters, das Ergebnisse an Security Hub CSPM sendet)
- Record state (Datensatzstatus)
- Region
- Ressourcen-Tag
- Schweregrad
- Workflow-Status

Standardmäßig werden Dashboard-Daten anhand der folgenden Kriterien gefiltert: `Workflow.Status` ist `NOTIFIED` oder`NEW`, und `RecordState` ist. `ACTIVE` Diese Kriterien werden über dem Dashboard unter dem Filterfeld angezeigt. Um diese Kriterien zu entfernen, wählen Sie X im Filtertoken für die Kriterien, die Sie entfernen möchten.

Wenn Sie Filterkriterien anwenden, die Sie erneut verwenden möchten, können Sie sie als Filtersatz speichern. Ein Filtersatz besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um sie erneut anzuwenden, wenn Sie Daten im Übersichts-Dashboard überprüfen. Sie können einen Filtersatz erstellen und speichern, der jedes der verfügbaren Felder mit Ausnahme der folgenden Felder verwendet: Anwendungs-ARN, Anwendungsname und Ressourcen-Tag.

Filtersätze erstellen und speichern

Gehen Sie wie folgt vor, um einen Filtersatz zu erstellen und zu speichern.

Um einen Filtersatz zu erstellen und zu speichern

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Geben Sie im Filterfeld über dem Übersichts-Dashboard die Filterkriterien für den Filtersatz ein.
4. Wählen Sie im Menü Filter löschen die Option Neuen Filtersatz speichern aus.
5. Geben Sie im Dialogfeld Filtersatz speichern einen Namen für den Filtersatz ein.
6. (Optional) Um den Filtersatz bei jedem Öffnen der Übersichtsseite standardmäßig zu verwenden, wählen Sie die Option, um ihn als Standardansicht festzulegen.
7. Wählen Sie Speichern.

Um zwischen den von Ihnen erstellten und gespeicherten Filtersätzen zu wechseln, verwenden Sie das Menü „Filtersatz auswählen“ über dem Übersichts-Dashboard. Wenn Sie einen Filtersatz auswählen, wendet Security Hub CSPM die Kriterien des Filtersatzes auf die Daten im Dashboard an.

Filtersätze aktualisieren oder löschen

Gehen Sie wie folgt vor, um einen vorhandenen Filtersatz zu aktualisieren oder zu löschen. Wenn Sie einen Filtersatz löschen, der derzeit als Standardansicht des Übersichts-Dashboards eingerichtet ist, wird Ihre Standardansicht auf die Standardansicht von Security Hub CSPM zurückgesetzt.

Um einen Filtersatz zu aktualisieren oder zu löschen

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Wählen Sie im Menü Wählen Sie einen Filtersatz über der Übersichtsseite den Filtersatz aus.
4. Führen Sie im Menü Filter löschen einen der folgenden Schritte aus:
   - Um den Filtersatz zu aktualisieren, wählen Sie Aktuellen Filtersatz aktualisieren. Geben Sie dann Ihre Änderungen in das angezeigte Dialogfeld ein.

- Um den Filtersatz zu löschen, wählen Sie Aktuellen Filtersatz löschen. Wählen Sie anschließend im daraufhin angezeigten Dialogfeld die Option Löschen.

Anpassen des Übersichts-Dashboards in Security Hub CSPM

Sie können das Übersichts-Dashboard auf der Security Hub CSPM-Konsole auf verschiedene Arten anpassen. Sie können zum Beispiel Widgets zum Dashboard hinzufügen und daraus entfernen. Sie können Widgets im Dashboard auch neu anordnen und ihre Größe ändern. Eine Liste der verfügbaren Widgets und eine Beschreibung der einzelnen Widgets finden Sie unter. Verfügbare Widgets für das Übersichts-Dashboard

Wenn Sie das Dashboard anpassen, wendet Security Hub CSPM Ihre Änderungen sofort an und speichert Ihre neuen Dashboard-Einstellungen. Ihre Änderungen gelten für Ihre Ansicht des Dashboards in allen AWS-Regionen Browsern.

Um das anzupassen Zusammenfassung Dashboard

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Führen Sie eine der folgenden Aktionen aus:

   - Um ein Widget hinzuzufügen, wählen Sie in der oberen rechten Ecke der Seite Widgets hinzufügen. Geben Sie in der Suchleiste den Titel des Widgets ein, das Sie hinzufügen möchten. Ziehen Sie dann das Widget an die gewünschte Position.
   - Um ein Widget zu entfernen, wählen Sie die drei Punkte in der oberen rechten Ecke des Widgets aus.
   - Um ein Widget zu verschieben, wählen Sie den Ziehpunkt in der oberen linken Ecke des Widgets und ziehen Sie das Widget dann an die gewünschte Position.
   - Um die Größe eines Widgets zu ändern, wählen Sie den Ziehpunkt zur Größenänderung in der unteren rechten Ecke des Widgets. Ziehen Sie den Rand des Widgets, bis das Widget Ihre bevorzugte Größe hat.

Um anschließend die ursprünglichen Einstellungen wiederherzustellen, wählen Sie „Auf Standardlayout zurücksetzen“ oben auf der Seite.

Regionale Grenzwerte für Security Hub CSPM

Einige AWS Security Hub CSPM-Funktionen sind nur in bestimmten Fällen verfügbar. AWS-Regionen In den folgenden Abschnitten werden diese regionalen Beschränkungen beschrieben. Eine vollständige Liste aller Regionen, in denen Security Hub CSPM derzeit verfügbar ist, finden Sie unter AWSSecurity Hub Hub-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Cross-Region Einschränkungen bei der Aggregation

In AWS GovCloud (US) Regions ist die regionsübergreifende Aggregation nur für Ergebnisse, Suchaktualisierungen und Erkenntnisse verfügbar. AWS GovCloud (US) Regions Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen den Regionen AWS GovCloud (US-East) und AWS GovCloud (US-West) zusammenfassen.

In den China Regionen ist die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Einblicke in die Regionen China verfügbar. Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen den Regionen China (Peking) und China (Ningxia) zusammenfassen.

Sie können eine Region, die standardmäßig deaktiviert ist, nicht als Ihre Aggregationsregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie im AWS -KontenverwaltungReferenzhandbuch unter AWS-RegionenIn Ihrem Konto aktivieren oder deaktivieren.

Verfügbarkeit von Integrationen nach Regionen

Einige Integrationen sind nicht in allen verfügbar. AWS-Regionen Auf der Security Hub CSPM-Konsole wird eine Integration nicht auf der Seite Integrationen angezeigt, wenn sie in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist.

Unterstützte Integrationen in den Regionen China (Peking) und China (Ningxia)

In den Regionen China (Peking) und China (Ningxia) unterstützt Security Hub CSPM nur die folgenden Integrationen mit: AWS-Services

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer

- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems ManagerOpsCenter
- AWS Systems ManagerPatch-Manager

In den Regionen China (Peking) und China (Ningxia) unterstützt Security Hub CSPM nur die folgenden Integrationen von Drittanbietern:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Unterstützte Integrationen inAWS GovCloud (US-East)undAWS GovCloud (US-West)Regionen

In den AWS GovCloud (US-West) Regionen AWS GovCloud (US-East) und unterstützt Security Hub CSPM nur die folgenden Integrationen mit: AWS-Services

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty

- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

In den AWS GovCloud (US-West) Regionen AWS GovCloud (US-East) und unterstützt Security Hub CSPM nur die folgenden Integrationen von Drittanbietern:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(nur verfügbar in AWS GovCloud (US-West))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer

- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Verfügbarkeit von Standards nach Regionen

Der vom AWS Control TowerService verwaltete Standard ist nur in den folgenden AWS-Regionen Bereichen verfügbarAWS Control Tower. Eine Liste der Regionen, die AWS Control Tower derzeit unterstützt werden, finden Sie unter How AWS-Regionen Work With AWS Control Tower im AWS Control TowerBenutzerhandbuch.

Der AWSResource Tagging-Standard ist in der Region Asien-Pazifik (Taipeh) nicht verfügbar.

Andere Sicherheitsstandards sind in allen Regionen verfügbar, in denen Security Hub CSPM derzeit verfügbar ist.

Verfügbarkeit von Kontrollen nach Regionen

Einige Security Hub CSPM-Steuerelemente sind nicht in allen verfügbar. AWS-Regionen Eine Liste der Steuerelemente, die nicht in jeder Region verfügbar sind, finden Sie unter. Regionale Beschränkungen der Security Hub CSPM-Steuerungen

Auf der Security Hub CSPM-Konsole erscheint ein Steuerelement nicht in der Kontrollliste, wenn es in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist. Die Ausnahme ist eine Aggregationsregion. Wenn Sie eine Aggregationsregion festlegen und sich bei dieser Region anmelden, werden in der Konsole Steuerelemente angezeigt, die in der Aggregationsregion oder einer oder mehreren verknüpften Regionen verfügbar sind.

Regionale Beschränkungen der Security Hub CSPM-Steuerungen

Einige AWS Security Hub CSPM-Steuerelemente sind nicht in allen verfügbar. AWS-Regionen Auf dieser Seite wird angegeben, welche Steuerelemente in bestimmten Regionen nicht verfügbar sind.

Auf der Security Hub CSPM-Konsole erscheint ein Steuerelement nicht in der Kontrollliste, wenn es in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist. Die Ausnahme ist eine Aggregationsregion. Wenn Sie eine Aggregationsregion festlegen und sich bei dieser Region

anmelden, werden in der Konsole Steuerelemente angezeigt, die in der Aggregationsregion oder einer oder mehreren verknüpften Regionen verfügbar sind.

AWS-Regionen

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Neuseeland)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Taipeh)
- Asien-Pazifik (Thailand)
- Asien-Pazifik (Tokio)
- Kanada (Zentral)
- Kanada West (Calgary)
- China (Peking)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europa (Milan)

- Europa (Paris)
- Europa (Spain)
- Europa (Stockholm)
- Europa (Zürich)
- Israel (Tel Aviv)
- Mexiko (Zentral)
- Middle East (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

USA Ost (Nord-Virginia)

Die folgenden Steuerelemente werden in der Region USA Ost (Nord-Virginia) nicht unterstützt.

- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

USA Ost (Ohio)

Die folgenden Steuerelemente werden in der Region USA Ost (Ohio) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden

- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

USA West (Nordkalifornien)

Die folgenden Steuerelemente werden in der Region USA West (Nordkalifornien) nicht unterstützt.

- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden

- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden

- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

USA West (Oregon)

Die folgenden Steuerelemente werden in der Region USA West (Oregon) nicht unterstützt.

- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Afrika (Kapstadt)

Die folgenden Steuerelemente werden in der Region Afrika (Kapstadt) nicht unterstützt.

- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden

- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden

- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Hongkong)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Hongkong) nicht unterstützt.

- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein

- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden

- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden

- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein

- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Hyderabad)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Hyderabad) nicht unterstützt.

- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden

- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden

- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben

- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden

- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein

- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Jakarta)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Jakarta) nicht unterstützt.

- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen

- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden

- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein

- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden

- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden

- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden

- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Malaysia)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Malaysia) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein

- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein

- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden

- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein

- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein

- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden

- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten

- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein

- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Melbourne)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Melbourne) nicht unterstützt.

- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben

- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden

- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben

- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden

- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Mumbai)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Mumbai) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden

- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Neuseeland)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Neuseeland) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation

- [APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert
- [APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden

- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden

- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein

- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden
- [ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben
- [ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren
- [ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen

- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden

- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden

- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby

- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein

- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden

- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation

- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.1] AWS Transfer Family Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Osaka)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Osaka) nicht unterstützt.

- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden

- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Seoul)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Seoul) nicht unterstützt.

- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden

- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden

- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Singapur)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Singapur) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Sydney)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Sydney) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden

- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Taipeh)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Taipeh) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.3] API Gateway REST API-Stufen sollten haben AWS X-Ray Ablaufverfolgung aktiviert
- [APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten mit Tags versehen werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Backup.5] AWS Backup Backup-Pläne sollten mit einem Tag versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- [CloudFormation.2] CloudFormation Stacks sollten markiert werden

- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden

- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.5] DynamoDB-Tabellen sollten markiert werden
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.10] Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert werden, die für den Amazon EC2-Service erstellt wurden

- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten mit Tags versehen werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten mit Tags versehen werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.13] ECS-Services sollten markiert werden
- [ECS.14] ECS-Cluster sollten markiert werden
- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden
- [ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben
- [ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren
- [ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden

- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starken AWS Config Dauer
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden

- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.1] Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein
- [ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben
- [ES.7] Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden
- [ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten markiert sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein

- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.23] IAM Access Analyzer-Analyzer sollten gekennzeichnet sein

- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden

- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein

- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren
- [RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden
- [RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden
- [RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden
- [RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden
- [RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] Snapshots von RDS-DB-Clustern sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden

- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren

- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys

- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.3] SNS-Themen sollten markiert werden
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein

- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden
- [Transfer.1] AWS Transfer Family Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Thailand)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Thailand) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden

- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein

- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden

- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind

- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden
- [ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben
- [ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren
- [ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken

- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein

- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein

- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein

- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation

- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.1] AWS Transfer Family Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Asien-Pazifik (Tokio)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Tokio) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Kanada (Zentral)

Die folgenden Steuerelemente werden in der Region Kanada (Mitte) nicht unterstützt.

- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden

- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Kanada West (Calgary)

Die folgenden Steuerelemente werden in der Region Kanada West (Calgary) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden

- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein

- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden

- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden

- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch

- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen

- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden

- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein

- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

China (Peking)

Die folgenden Steuerelemente werden in der Region China (Peking) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein

- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten gekennzeichnet sein
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein

- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden

- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein

- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

China (Ningxia)

Die folgenden Steuerelemente werden in der Region China (Ningxia) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden

- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden

- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen

- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten gekennzeichnet sein
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden

- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein

- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen

- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein

- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Frankfurt)

Die folgenden Steuerelemente werden in der Region Europa (Frankfurt) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden

- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Irland)

Die folgenden Steuerelemente werden in der Region Europa (Irland) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (London)

Die folgenden Steuerelemente werden in der Region Europa (London) nicht unterstützt.

- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden

- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Milan)

Die folgenden Steuerelemente werden in der Region Europa (Mailand) nicht unterstützt.

- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden

- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden

- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Europa (Paris)

Die folgenden Steuerelemente werden in der Region Europa (Paris) nicht unterstützt.

- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein

- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden

- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Europa (Spain)

Die folgenden Steuerelemente werden in der Region Europa (Spanien) nicht unterstützt.

- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden

- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden

- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht so konfiguriert werden, dass sie öffentlich wiederherstellbar sind
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS

- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden

- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein

- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Europa (Stockholm)

Die folgenden Steuerelemente werden in der Region Europa (Stockholm) nicht unterstützt.

- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein

- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Europa (Zürich)

Die folgenden Steuerelemente werden in der Region Europa (Zürich) nicht unterstützt.

- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein

- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden

- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden

- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein

- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Israel (Tel Aviv)

Die folgenden Kontrollen werden in der Region Israel (Tel Aviv) nicht unterstützt.

- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden

- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden

- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [ELB.2] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern

- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden

- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein

- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.29] Snapshots von RDS-DB-Clustern sollten mit Tags versehen werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden

- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Mexiko (Zentral)

Die folgenden Steuerelemente werden in der Region Mexiko (Zentral) nicht unterstützt.

- [ACM.1] Importiert und ACM-issued Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation

- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden

- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein

- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die EC2-Transit-Gateway-Routentabellen sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen
- [EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden
- [EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden
- [EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden

- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein
- [EC2.172] Die EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.182] Einstellungen für den öffentlichen Zugriff blockieren sollten für Amazon EBS-Snapshots aktiviert sein
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [ECS.18] ECS-Aufgabendefinitionen sollten die Verschlüsselung während der Übertragung für EFS-Volumes verwenden
- [ECS.19] ECS-Kapazitätsanbieter sollten den Managed Termination Protection aktiviert haben
- [ECS.20] ECS-Aufgabendefinitionen sollten Nicht-Root-Benutzer in Linux-Container-Definitionen konfigurieren
- [ECS.21] ECS-Aufgabendefinitionen sollten Benutzer ohne Administratorrechte in Windows-Containerdefinitionen konfigurieren
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen
- [EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein
- [EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein
- [GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.7] Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben

- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden

- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoT.4]AWS IoT CoreAutorisierer sollten markiert werden
- [IoT.5]AWS IoT CoreRollenaliase sollten mit Tags versehen werden
- [IoT.6]AWS IoT CoreRichtlinien sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert

- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

- [RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden

- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.22] S3-Buckets für allgemeine Zwecke sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden

- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Middle East (Bahrain)

Die folgenden Steuerelemente werden in der Region Naher Osten (Bahrain) nicht unterstützt.

- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden

- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.10] Datenspeicher für Ereignisse in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden

- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.20] Beide VPN-Tunnel für ein AWS Site-to-Site Die VPN-Verbindung sollte bestehen
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ
- [FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein

- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden
- [RDS.42] RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein

- [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein

- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Naher Osten (VAE)

Die folgenden Steuerelemente werden in der Region Naher Osten (VAE) nicht unterstützt.

- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFormation.3] CloudFormation Stacks sollte der Kündigungsschutz aktiviert sein
- [CloudFormation.4] CloudFormation Stacks sollten zugeordnete Servicerollen haben
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden

- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [Detective.1] Graphen zum Verhalten von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben
- [DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben
- [DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein
- [DMS.13] DMS-Replikationsinstanzen sollten so konfiguriert werden, dass sie mehrere Availability Zones verwenden
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.14] Sicherheitsgruppen sollten ab Version 0.0.0 keinen Zugriff zulassen. 0/0 oder: :/0 zu Port 3389

- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [EC2.180] Bei EC2-Netzwerkschnittstellen sollte die Überprüfung aktiviert sein source/destination
- [EC2.181] EC2-Startvorlagen sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.183] EC2-VPN-Verbindungen sollten das IKEv2-Protokoll verwenden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EKS.9] EKS-Knotengruppen sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden
- [ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein

- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein
- [Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden

- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.7] Lambda-Funktionen sollten haben AWS X-Ray aktives Tracing aktiviert
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen

- [Redshift.18] Für Redshift-Cluster sollten Multi-AZ Bereitstellungen aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden

- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Südamerika (São Paulo)

Die folgenden Steuerelemente werden in der Region Südamerika (São Paulo) nicht unterstützt.

- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden

- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden

- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoT.1]AWS IoT Device DefenderSicherheitsprofile sollten markiert werden
- [IoT.2]AWS IoT CoreMaßnahmen zur Schadensbegrenzung sollten mit einem Tag versehen werden
- [IoT.3]AWS IoT CoreDimensionen sollten mit Tags versehen werden
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden

- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

AWS GovCloud (US-East)

Die folgenden Steuerelemente werden in der AWS GovCloud (US-East) Region nicht unterstützt.

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden

- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden
- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen

- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden
- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden
- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [Connect.2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden
- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben

- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein

- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein

- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.16] SageMaker Modelle sollten eine private Registrierung in VPC für primäre Container verwenden
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SageMaker.19] SageMaker Modelle sollten eine private Registrierung in VPC für Inferenz-Pipelines mit mehreren Containern verwenden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten

- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein
- [WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden
- [WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

AWS GovCloud (US-West)

Die folgenden Steuerelemente werden in der AWS GovCloud (US-West) Region nicht unterstützt.

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto
- [Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation
- [APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben
- [APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden
- [APIGateway.10] API Gateway V2-Integrationen sollten HTTPS für private Verbindungen verwenden
- [APIGateway.11] API Gateway Gateway-Domainnamen sollten empfohlene Sicherheitsrichtlinien verwenden
- [Amplify.1] Amplify-Apps sollten markiert werden
- [Amplify.2] Amplify-Zweige sollten markiert werden
- [AppConfig.1]AWS AppConfigAnwendungen sollten markiert werden
- [AppConfig.2]AWS AppConfigKonfigurationsprofile sollten mit Tags versehen werden

- [AppConfig.3]AWS AppConfigUmgebungen sollten markiert werden
- [AppConfig.4]AWS AppConfigErweiterungszuordnungen sollten mit Tags versehen werden
- [AppFlow.1] AppFlow Amazon-Flows sollten markiert werden
- [AppRunner.1] App Runner-Dienste sollten markiert sein
- [AppRunner.2] App Runner VPC-Konnektoren sollten markiert werden
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Backup.4] AWS Backup Berichtspläne sollten mit Tags versehen werden
- [Batch.1] Batch-Job-Warteschlangen sollten markiert werden
- [Batch.2] Richtlinien zur Batch-Planung sollten markiert werden
- [Batch.3] Batch-Computing-Umgebungen sollten markiert werden
- [Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden
- [BedrockAgentCore.1] AgentCore Bedrock-Laufzeiten sollten mit dem VPC-Netzwerkmodus konfiguriert werden
- [BedrockAgentCore.2] Bedrock AgentCore Gateways sollten eine Autorisierung für eingehende Anfragen benötigen
- [BedrockAgentCore.3] Bedrock AgentCore Memory sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway sollte verschlüsselt und vom Kunden verwaltet werden AWS KMS keys
- [BedrockAgentCore.5] AgentCore Benutzerdefinierte Bedrock-Browser sollten den öffentlichen Netzwerkmodus nicht verwenden

- [BedrockAgentCore.6] Für AgentCore benutzerdefinierte Bedrock-Browser sollte die Sitzungsaufzeichnung aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten markiert werden
- [CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden
- [CloudFront.16] CloudFront Distributionen sollten die Origin-Zugriffskontrolle für die URL-Ursprünge der Lambda-Funktion verwenden
- [CloudFront.17] CloudFront Distributionen sollten vertrauenswürdige Schlüsselgruppen für signierte URLs und Cookies verwenden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten markiert werden
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild.4] CodeBuild Projektumgebungen sollten über eine Protokollierung verfügen AWS Config Dauer
- [CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden

- [CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden
- [Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein
- [Cognito.3] Passwortrichtlinien für Cognito-Benutzerpools sollten starke Konfigurationen haben
- [Cognito.4] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die benutzerdefinierte Authentifizierung aktiviert sein
- [Cognito.5] MFA sollte für Cognito-Benutzerpools aktiviert sein
- [Cognito.6] In Cognito-Benutzerpools sollte der Löschschutz aktiviert sein
- [Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden
- [DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden
- [DMS.2] DMS-Zertifikate sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.21] Netzwerk-ACLs sollten ab Version 0.0.0 keinen Zugriff mehr zulassen. 0/0 zu Port 22 oder Port 3389
- [EC2.22] Unbenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden

- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanforderungen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden
- [EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden
- [EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.173] EC2 Spot Fleet-Anfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen
- [EC2.174] EC2-DHCP-Optionssätze sollten markiert werden
- [EC2.175] EC2-Startvorlagen sollten mit Tags versehen werden
- [EC2.176] EC2-Präfixlisten sollten mit Tags versehen werden
- [EC2.177] EC2-Traffic-Mirror-Sitzungen sollten mit Tags versehen werden
- [EC2.178] EC2-Traffic-Spiegelfilter sollten mit Tags versehen werden
- [EC2.179] EC2-Traffic-Mirror-Ziele sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Aufgabendefinitionen sollten Container so konfigurieren, dass sie auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sind
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.13] Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.21] Anwendungs- und Network Load Balancer Balancer-Zielgruppen sollten verschlüsselte Health Check-Protokolle verwenden
- [ELB.22] ELB-Zielgruppen sollten verschlüsselte Transportprotokolle verwenden
- Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein
- [ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein
- [ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein
- [EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden
- [EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden

- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in Logs sollte aktiviert sein CloudWatch
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein
- [FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten markiert werden
- [FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden
- [FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten markiert sein
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein
- [GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein
- [GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein
- [IAM.6] Hardware-MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein
- [Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein
- [IoTSiteWise.1]AWS SiteWise IoT-Asset-Modelle sollten markiert werden
- [IoTSiteWise.2]AWS SiteWise IoT-Dashboards sollten mit Tags versehen werden
- [IoTSiteWise.3]AWS SiteWise IoT-Gateways sollten markiert werden

- [IoTSiteWise.4]AWS SiteWise IoT-Portale sollten mit Tags versehen werden
- [IoTSiteWise.5]AWS SiteWise IoT-Projekte sollten markiert werden
- [IoTTwinMaker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden
- [IoTTwinMaker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden
- [IoTTwinMaker.3] AWS TwinMaker IoT-Szenen sollten markiert werden
- [IoTTwinMaker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden
- [IoTWireless.1]AWSIoT-Wireless-Multicast-Gruppen sollten markiert werden
- [IoTWireless.2]AWSIoT-Wireless-Dienstprofile sollten markiert werden
- [IoTWireless.3]AWSIoT FUOTA-Aufgaben sollten markiert werden
- [IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden
- [IVS.2] IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden
- [IVS.3] IVS-Kanäle sollten markiert werden
- [Keyspaces.1] Amazon Keyspaces-Keyspaces sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden
- [MSK.5] Für MSK-Konnektoren sollte die Protokollierung aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

- [Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete Drop oder Forward sein
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete Drop oder Forward sein
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [Opensearch.4] OpenSearch Die Protokollierung von Domain-Fehlern in Logs sollte aktiviert sein CloudWatch
- [Opensearch.5] Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben
- Bei [Opensearch.7] OpenSearch Domänen sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein
- [PCA.2] AWS Private Zertifizierungsstellen sollten markiert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein
- [RDS.43] RDS-DB-Proxys sollten TLS-Verschlüsselung für Verbindungen erfordern
- [RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Auditprotokollierung aktiviert sein
- [RDS.47] RDS für PostgreSQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.48] RDS für MySQL-DB-Cluster sollten so konfiguriert sein, dass Tags in DB-Snapshots kopiert werden
- [RDS.50] Für RDS-DB-Cluster sollte ein ausreichender Aufbewahrungszeitraum für Backups festgelegt sein
- [RDS.51] Globale RDS-Cluster sollten auf einer unterstützten Aurora MySQL-Version laufen
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den Standard-Admin-Benutzernamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden
- [RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden
- [RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein
- [RedshiftServerless.3] Redshift Serverless-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten
- [RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch
- [Route53.1] Route 53-Gesundheitschecks sollten markiert werden
- [Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden

- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Für S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein
- [S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden
- [SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden
- [SageMaker.9] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- Bei Auftragsdefinitionen zur Erläuterung des SageMaker Modells [SageMaker.10] sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.11] Bei Auftragsdefinitionen SageMaker zur Datenqualität sollte die Netzwerkisolierung aktiviert sein
- Bei Auftragsdefinitionen für [SageMaker.12] SageMaker Model Bias sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.13] Bei Auftragsdefinitionen in SageMaker Modellqualität sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.14] In den SageMaker Überwachungsplänen sollte die Netzwerkisolierung aktiviert sein
- [SageMaker.15] Bei Jobdefinitionen mit SageMaker Modellverzerrung sollte die Verschlüsselung des Datenverkehrs zwischen Containern aktiviert sein
- [SageMaker.17] Offline-Shops für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys

- [SageMaker.18] Onlineshops mit Standardspeicher für SageMaker Featuregruppen sollten verschlüsselt werden mit AWS KMS keys
- [SES.3] In SES-Konfigurationssätzen sollte TLS für das Senden von E-Mails aktiviert sein
- [SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen
- [SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [SSM.5] SSM-Dokumente sollten mit Tags versehen werden
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Step Functions Functions-Aktivitäten sollten markiert werden
- [Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden
- [Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein
- [Transfer.6] Steckverbinder der Transfer Family sollten gekennzeichnet sein
- [Transfer.7] Familienprofile übertragen sollten markiert werden
- [WAF.1] AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein

Security Hub CSPM-Ressourcen erstellen mit CloudFormation

AWSSecurity Hub CSPM lässt sich in einen Dienst integrierenAWS CloudFormation, der Ihnen hilft, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine

Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. Automatisierungsregeln) und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwendenCloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Security Hub CSPM-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren Regionen bereitAWS-Konten.

Security Hub CSPM undCloudFormationVorlagen

Um Ressourcen für Security Hub CSPM und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie wissen, wie CloudFormationVorlagen funktionieren. Vorlagen sind Textdateien im JSON- oder YAML-Format. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation Stacks bereitstellen möchten.

Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. CloudFormation Weitere Informationen finden Sie unter Was ist CloudFormation Designer? im AWS CloudFormationBenutzerhandbuch.

Sie können CloudFormation Vorlagen für die folgenden Typen von Security Hub CSPM-Ressourcen erstellen:

- Security Hub CSPM aktivieren
- Benennen des delegierten Security Hub CSPM-Administrators für eine Organisation
- Geben Sie an, wie Ihre Organisation in Security Hub CSPM konfiguriert ist
- Aktivierung eines Sicherheitsstandards
- Aktivierung der regionsübergreifenden Aggregation
- Erstellen Sie eine zentrale Konfigurationsrichtlinie und verknüpfen Sie sie mit Konten, Organisationseinheiten (OUs) oder dem Stamm
- Einen benutzerdefinierten Einblick erstellen
- Eine Automatisierungsregel erstellen
- Anpassen der Steuerparameter
- Abonnieren Sie eine Produktintegration eines Drittanbieters

Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Ressourcen, finden Sie in der Referenz zum AWS Security Hub CSPM-Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

Erfahren Sie mehr überCloudFormation

Weitere Informationen CloudFormation finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormationBenutzerhandbuch
- CloudFormationAPI Reference
- AWS CloudFormationBenutzerhandbuch für die Befehlszeilenschnittstelle

Abonnieren von Security Hub CSPM-Ankündigungen mit Amazon SNS

Dieser Abschnitt enthält Informationen zum Abonnieren von AWS Security Hub CSPM-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen über Security Hub CSPM zu erhalten.

Nach dem Abonnieren erhalten Sie Benachrichtigungen über die folgenden Ereignisse (beachten Sie die entsprechenden Ereignisse): `AnnouncementType`

- `NEW_STANDARDS_CONTROLS`— Neue Security Hub CSPM-Steuerungen oder -Standards wurden hinzugefügt.
- `RETIRED_STANDARDS_CONTROLS`— Bestehende Security Hub CSPM-Kontrollen oder -Standards wurden eingestellt.

Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Sie können die Ankündigungen von Security Hub CSPM in allen Bereichen abonnieren, in AWS-Regionendenen Security Hub CSPM verfügbar ist.

Ein Benutzer muss über `Subscribe` Berechtigungen verfügen, um ein Amazon SNS SNS-Thema zu abonnieren. Sie können dies mit Amazon SNS SNS-Richtlinien, IAM-Richtlinien oder beidem erreichen. Weitere Informationen finden Sie unter IAM- und Amazon SNS SNS-Richtlinien zusammen im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Security Hub CSPM sendet Amazon SNS SNS-Ankündigungen über Updates für den Security Hub CSPM-Service an alle Abonnenten. AWS-Konto Um Benachrichtigungen über

Security Hub CSPM-Ergebnisse zu erhalten, siehe. Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM

Sie können eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange für ein Amazon SNS SNS-Thema abonnieren, müssen jedoch einen Amazon SNS SNS-Thema Amazon Resource Name (ARN) verwenden, der sich in derselben Region befindet. Weitere Informationen finden Sie unter Abonnieren einer Warteschlange für ein Amazon SNS im Amazon Simple Queue Service Developer Guide.

Sie können auch eine AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Sie Benachrichtigungen erhalten. Weitere Informationen, einschließlich Beispielfunktionscode, finden Sie unter Tutorial: Using AWS Lambda with Amazon Simple Notification Service im AWS LambdaEntwicklerhandbuch.

Die Amazon SNS SNS-Themen-ARNs für jede Region lauten wie folgt.

AWS-Region	ARN des Amazon-SNS-Themas
US East (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
USA Ost (Nord-Virginia)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
USA West (Nordkalifornien)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
USA West (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
Africa (Cape Town)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Asien-Pazifik (Hongkong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asien-Pazifik (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Asien-Pazifik (Jakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asien-Pazifik (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asien-Pazifik (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asien-Pazifik (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asien-Pazifik (Singapur)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asien-Pazifik (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asien-Pazifik (Tokio)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Canada (Central)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
China (Peking)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
China (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europe (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Europa (Irland)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europa (London)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europa (Milan)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Europa (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Europa (Spain)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Europa (Stockholm)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europa (Zürich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Middle East (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Naher Osten (VAE)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Südamerika (São Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (US-East)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (US-West)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Die Nachrichten sind in der Regel in allen Regionen innerhalb einer Partition identisch. Sie können also eine Region in jeder Partition abonnieren, um Ankündigungen zu erhalten, die sich auf alle Regionen in dieser Partition auswirken. Ankündigungen, die mit Mitgliedskonten verknüpft sind, werden nicht im Administratorkonto repliziert. Daher verfügt jedes Konto, einschließlich des

Administratorkontos, nur über eine Kopie jeder Ankündigung. Sie können entscheiden, welches Konto Sie verwenden möchten, um Security Hub CSPM-Ankündigungen zu abonnieren.

Informationen zu den Kosten für das Abonnieren von Security Hub CSPM-Ankündigungen finden Sie unter Amazon SNS SNS-Preise.

Security Hub CSPM-Ankündigungen abonnieren (Konsole)

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie in der Liste Region die Region aus, in der Sie Security Hub CSPM-Ankündigungen abonnieren möchten. In diesem Beispiel wird die Region `us-west-2` verwendet.
3. Wählen Sie im Navigationsbereich Subscriptions (Abonnements) und dann Create subscription (Abonnement erstellen) aus.
4. Geben Sie den Themen-ARN in das Feld Themen-ARN ein. Beispiel, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Wählen Sie unter Protokoll aus, wie Sie Security Hub CSPM-Ankündigungen erhalten möchten. Wenn Sie E-Mail wählen, geben Sie für Endpoint die E-Mail-Adresse ein, die Sie für den Empfang von Ankündigungen verwenden möchten.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Abonnieren von Security Hub CSPM-Ankündigungen (AWS CLI)

1. Führen Sie den folgenden Befehl aus:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Amazon-SNS-Nachrichtenformat

Die folgenden Beispiele zeigen Security Hub CSPM-Ankündigungen von Amazon SNS zur Einführung neuer Sicherheitskontrollen. Der Nachrichteninhalt variiert je nach Art der Ankündigung, aber das Format ist für alle Ankündigungstypen gleich. Optional kann ein `Link` Feld mit Details zur Ankündigung hinzugefügt werden.

Beispiel: Security Hub CSPM-Ankündigung für neue Kontrollen (E-Mail-Protokoll)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to theAWSFoundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront
 (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27),
 Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic
 Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon
 Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service
 (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1),AWS Network Firewall(NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. "
}
```

Beispiel: Security Hub CSPM-Ankündigung für neue Kontrollen (E-Mail-JSON-Protokoll)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":
\"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard\",\"Description\":\"We have added 36 new
 controls to theAWSFoundational Security Best Practices standard. These
 include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4,
```

```
 AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront (CloudFront.10),
 Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic
 Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service
 (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System
 (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2),
 Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1),AWS
 Network Firewall(NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon
 OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Security Hub CSPM deaktivieren

Sie können AWS Security Hub CSPM mithilfe der Security Hub CSPM-Konsole oder der Security Hub Hub-API deaktivieren. Wenn Sie Security Hub CSPM deaktivieren, können Sie es später wieder aktivieren.

Wenn Ihre Organisation die zentrale Konfiguration verwendet, kann der delegierte Security Hub CSPM-Administrator Konfigurationsrichtlinien erstellen, die Security Hub CSPM für bestimmte Konten und Organisationseinheiten (OUs) deaktivieren und Security Hub CSPM für andere aktivieren. Die Konfigurationsrichtlinien wirken sich auf die Heimatregion und alle verknüpften Regionen aus. Weitere Informationen finden Sie unter Grundlegendes zur zentralen Konfiguration in Security Hub CSPM.

Wenn Sie Security Hub CSPM für ein Konto deaktivieren, passiert Folgendes:

- Alle Security Hub CSPM-Standards und -Kontrollen sind für das Konto deaktiviert.
- Security Hub CSPM beendet die Generierung, Aktualisierung und Erfassung von Ergebnissen für das Konto.
- Nach 30 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen archivierten Ergebnisse für das Konto. Die Ergebnisse können mit Security Hub CSPM nicht wiederhergestellt werden.
- Nach 90 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen aktiven Ergebnisse für das Konto. Die Ergebnisse können mit Security Hub CSPM nicht wiederhergestellt werden.
- Nach 90 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen Insights und Security Hub CSPM-Konfigurationseinstellungen für das Konto. Die Daten und Einstellungen können nicht wiederhergestellt werden.

Um bestehende Ergebnisse beizubehalten, können Sie die Ergebnisse in einen S3-Bucket exportieren, bevor Sie Security Hub CSPM deaktivieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter Verwendung EventBridge für automatische Reaktionen und Problembehebungen.

Wenn Sie Security Hub CSPM innerhalb von 90 Tagen nach der Deaktivierung für ein Konto erneut aktivieren, erhalten Sie wieder Zugriff auf bestehende aktive Ergebnisse sowie auf Einblicke und Security Hub CSPM-Konfigurationseinstellungen für das Konto. Wenn Sie Security Hub CSPM innerhalb von 30 Tagen erneut aktivieren, erhalten Sie auch wieder Zugriff auf bestehende archivierte Ergebnisse für das Konto. Bestehende Ergebnisse können jedoch ungenau sein, da sie den Zustand Ihrer AWS Umgebung widerspiegeln, als Sie Security Hub CSPM deaktiviert haben. Wenn Sie einzelne Standards und Kontrollen wieder aktivieren, generiert Security Hub CSPM außerdem möglicherweise zunächst doppelte Ergebnisse für bestimmte AWS Ressourcen, je nachdem, welche Standards und Kontrollen Sie aktivieren. Aus diesen Gründen empfehlen wir Ihnen, einen der folgenden Schritte durchzuführen:

- Ändern Sie den Workflow-Status aller vorhandenen Ergebnisse auf „`RESOLVED`Bevor Sie Security Hub CSPM deaktivieren“. Weitere Informationen finden Sie unter Den Workflow-Status von Ergebnissen festlegen.
- Deaktivieren Sie alle Standards mindestens sechs Tage vor der Deaktivierung von Security Hub CSPM. Security Hub CSPM archiviert dann alle vorhandenen Ergebnisse nach bestem Wissen und Gewissen, in der Regel innerhalb von drei bis fünf Tagen. Weitere Informationen finden Sie unter Deaktivierung eines Standards.

In den folgenden Fällen können Sie Security Hub CSPM nicht deaktivieren:

- Ihr Konto ist das delegierte Security Hub CSPM-Administratorkonto für eine Organisation. Wenn Sie die zentrale Konfiguration verwenden, können Sie keine Konfigurationsrichtlinie zuordnen, die Security Hub CSPM für das delegierte Administratorkonto deaktiviert. Die Zuordnung kann für andere Konten erfolgreich sein, aber Security Hub CSPM wendet die Richtlinie nicht auf das delegierte Administratorkonto an.
- Ihr Konto ist auf Einladung ein Security Hub CSPM-Administratorkonto, und Sie haben Mitgliedskonten. Bevor Sie Security Hub CSPM deaktivieren können, müssen Sie die Verknüpfung aller Ihrer Mitgliedskonten aufheben. Um zu erfahren wie dies geht, vgl. the section called “Aufheben der Zuordnung von Mitgliedskonten”.

Bevor der Besitzer eines Mitgliedskontos Security Hub CSPM deaktivieren kann, muss das Konto von seinem Administratorkonto getrennt werden. Bei einem Organisationskonto kann nur das Administratorkonto die Zuordnung zu einem Mitgliedskonto aufheben. Weitere Informationen finden Sie unter the section called “Aufheben der Zuordnung von Mitgliedskonten der Organisation”. Bei einem manuell eingeladenen Konto kann entweder das Administratorkonto oder das Mitgliedskonto die Zuordnung des Kontos aufheben. Für weitere Informationen siehe the section called “Aufheben der Zuordnung von Mitgliedskonten” oder the section called “Trennung von einem Administratorkonto”. Eine Trennung der Zuordnung ist nicht erforderlich, wenn Sie die zentrale Konfiguration verwenden, da der Security Hub CSPM-Administrator eine Richtlinie erstellen kann, die Security Hub CSPM für bestimmte Mitgliedskonten deaktiviert.

Wenn Sie Security Hub CSPM für ein Konto deaktivieren, ist es nur aktuell deaktiviert. AWS-Region Wenn Sie jedoch die zentrale Konfiguration verwenden, um Security Hub CSPM für bestimmte Konten zu deaktivieren, ist es in der Heimatregion und allen verknüpften Regionen deaktiviert.

Um Security Hub CSPM zu deaktivieren, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten.

Security Hub CSPM console

Gehen Sie wie folgt vor, um Security Hub CSPM mithilfe der Konsole zu deaktivieren.

So deaktivieren Sie Security Hub CSPM

1. Öffnen Sie die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Klicken Sie im Navigationsbereich unter Settings auf General.

3. Wählen Sie im Abschnitt Security Hub CSPM deaktivieren die Option Security Hub CSPM deaktivieren aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Disable Security Hub CSPM.

Security Hub API

Verwenden Sie den DisableSecurityHubBetrieb der Security Hub-API, um Security Hub CSPM programmgesteuert zu deaktivieren. AWS Oder, wenn Sie den verwenden, führen Sie den Befehl AWS CLI disable-security-hub aus. Beispielsweise deaktiviert der folgende Befehl Security Hub CSPM in der aktuellen Version: AWS-Region

```
$ aws securityhub disable-security-hub
```

Sicherheit bei AWS Security Hub CSPM

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-partyAuditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS Compliance-Programme. Weitere Informationen zu den Compliance-Programmen für AWS Security Hub CSPM finden Sie unter Durch das Compliance-Programm abgedeckte AWS -Services.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Security Hub CSPM anwenden können. In den folgenden Themen erfahren Sie, wie Sie Security Hub CSPM konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu

erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Security Hub CSPM-Ressourcen zu überwachen und zu sichern.

Topics

- Datenschutz in AWS Security Hub CSPM
- AWS Identity and Access Management für Security Hub CSPM
- Konformitätsprüfung für AWS Security Hub CSPM
- Resilienz in AWS Security Hub
- Sicherheit der Infrastruktur in AWS Security Hub CSPM
- AWS Security Hub CSPM und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Datenschutz in AWS Security Hub CSPM

Für den Datenschutz in AWS Security Hub CSPM gilt das Modell der geteilten Verantwortung das von AWS . Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.

- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Security Hub CSPM oder einem anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Security Hub CSPM ist ein Serviceangebot für mehrere Mandanten. Um den Datenschutz zu gewährleisten, verschlüsselt Security Hub CSPM ruhende Daten und Daten, die zwischen Komponentendiensten übertragen werden.

AWS Identity and Access Management für Security Hub CSPM

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Security Hub Hub-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Security Hub mit IAM
- Identity-based Richtlinienbeispiele für AWS Security Hub CSPM
- Service-linked Rollen für AWS Security Hub CSPM
- AWS verwaltete Richtlinien für Security Hub
- Fehlerbehebung AWS Security Hub CSPM Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung AWS Security Hub CSPM Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Security Hub mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinienbeispiele für AWS Security Hub CSPM).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Security Hub mit IAM

Bevor Sie AWS Identity and Access Management (IAM) zur Zugriffsverwaltung verwenden, sollten Sie sich darüber AWS Security Hub CSPM informieren, welche IAM-Funktionen mit Security Hub CSPM verwendet werden können.

IAM-Funktionen, die Sie mit verwenden können AWS Security Hub CSPM

IAM-Feature	Security Hub CSPM-Unterstützung
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Ja
Zugriffskontrolllisten (ACLs)	Nein

IAM-Feature	Security Hub CSPM-Unterstützung
Attribute-based Zugriffskontrolle (ABAC) — Tags in Richtlinien	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie Security Hub CSPM und andere mit den meisten IAM-Funktionen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese funktionieren mit IAM.

Identity-based Richtlinien für Security Hub CSPM

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Security Hub CSPM unterstützt identitätsbasierte Richtlinien. Weitere Informationen finden Sie unter Identity-based Richtlinienbeispiele für AWS Security Hub CSPM.

Resource-based Richtlinien für Security Hub CSPM

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Security Hub CSPM unterstützt keine ressourcenbasierten Richtlinien. Sie können eine IAM-Richtlinie nicht direkt an eine Security Hub-CSPM-Ressource anhängen.

Richtlinienaktionen für Security Hub CSPM

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Richtlinienaktionen in Security Hub CSPM verwenden das folgende Präfix vor der Aktion:

```
securityhub:
```

Um einem Benutzer beispielsweise die Erlaubnis zu erteilen, Security Hub CSPM zu aktivieren, was eine Aktion ist, die dem `EnableSecurityHub` Betrieb der Security Hub CSPM-API entspricht, nehmen Sie die `securityhub:EnableSecurityHub` Aktion in ihre Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Security Hub CSPM definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

```
"Action": "securityhub:EnableSecurityHub"
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Beispiel:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Sie können auch mehrere Aktionen mithilfe von Platzhaltern (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

```
"Action": "securityhub:Get*"
```

Als bewährte Methode sollten Sie jedoch Richtlinien erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die zum Ausführen einer bestimmten Aufgabe erforderlich sind.

Der Benutzer muss Zugriff auf den `DescribeStandardsControl` Vorgang haben, um auf `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, und `ListStandardsControlAssociations` zugreifen zu können.

Der Benutzer muss Zugriff auf den `UpdateStandardsControls` Vorgang haben, um Zugriff auf`BatchUpdateStandardsControlAssociations`, und zu haben`UpdateSecurityControl`.

Eine Liste der Security Hub CSPM-Aktionen finden Sie unter Actions defined by AWS Security Hub CSPM in der Service Authorization Reference. Beispiele für Richtlinien, die Security Hub CSPM-Aktionen spezifizieren, finden Sie unter. Identity-based Richtlinienbeispiele für AWS Security Hub CSPM

Richtlinienressourcen für Security Hub CSPM

Unterstützt Richtlinienressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen

(ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Security Hub CSPM definiert die folgenden Ressourcentypen:

- Hub (Hub)
- Produkt
- Aggregator für die Suche, auch als regionsübergreifender Aggregator bezeichnet
- Automatisierungsregel
- Konfigurationsrichtlinie

Sie können diese Ressourcentypen mithilfe von ARNs in Richtlinien angeben.

Eine Liste der Security Hub CSPM-Ressourcentypen und die jeweilige ARN-Syntax finden Sie unter Ressourcentypen definiert von AWS Security Hub CSPM in der Service Authorization Reference. Informationen darüber, welche Aktionen Sie für jeden Ressourcentyp angeben können, finden Sie unter Aktionen definiert von AWS Security Hub CSPM in der Service Authorization Reference. Beispiele für Richtlinien, die Ressourcen spezifizieren, finden Sie unterIdentity-based Richtlinienbeispiele für AWS Security Hub CSPM.

Schlüssel für Richtlinienbedingungen für Security Hub CSPM

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Security Hub CSPM-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Security Hub CSPM in der Service Authorization Reference. Informationen zu den Aktionen

und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von. AWS Security Hub CSPM Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unterIdentity-based Richtlinienbeispiele für AWS Security Hub CSPM.

Zugriffskontrolllisten (ACLs) in Security Hub CSPM

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Security Hub CSPM unterstützt keine ACLs, was bedeutet, dass Sie keine ACL an eine Security Hub CSPM-Ressource anhängen können.

Attribute-based Zugriffskontrolle (ABAC) mit Security Hub CSPM

Unterstützt ABAC (Tags in Richtlinien): Ja

Attribute-based Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Sie können Tags an Security Hub CSPM-Ressourcen anhängen. Sie können den Zugriff auf Ressourcen auch kontrollieren, indem Sie Tag-Informationen im `Condition` Element einer Richtlinie angeben.

Informationen zum Taggen von Security Hub CSPM-Ressourcen finden Sie unter. Kennzeichnen von Security Hub Hub-Ressourcen Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf

eine Ressource anhand von Tags steuert, finden Sie unter. Identity-based Richtlinienbeispiele für AWS Security Hub CSPM

Temporäre Anmeldeinformationen mit Security Hub CSPM verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen GetFederationToken.

Security Hub CSPM unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Security Hub CSPM weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Principals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Beispielsweise sendet Security Hub CSPM FAS-Anfragen an Downstream, AWS-Services wenn Sie Security Hub CSPM in Organizations integrieren AWS Organizations und das delegierte Security Hub CSPM-Administratorkonto für eine Organisation festlegen.

Für andere Aufgaben verwendet Security Hub CSPM eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unter. Service-linked Rollen für AWS Security Hub CSPM

Servicerollen für Security Hub CSPM

Security Hub CSPM übernimmt oder verwendet keine Servicerollen. Um Aktionen in Ihrem Namen durchzuführen, verwendet Security Hub CSPM eine dienstbezogene Rolle. Einzelheiten zu dieser Rolle finden Sie unter. Service-linked Rollen für AWS Security Hub CSPM

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu Betriebsproblemen bei der Verwendung von Security Hub CSPM führen. Bearbeiten Sie Servicerollen nur, wenn Security Hub CSPM Sie dazu anleitet.

Service-linked Rollen für Security Hub CSPM

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Security Hub CSPM verwendet eine dienstbezogene Rolle, um Aktionen in Ihrem Namen durchzuführen. Einzelheiten zu dieser Rolle finden Sie unter. Service-linked Rollen für AWS Security Hub CSPM

Identity-based Richtlinienbeispiele für AWS Security Hub CSPM

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Security Hub CSPM-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder AWS API ausführen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien
- Verwenden der Security Hub CSPM-Konsole
- Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Beispiel: Erlauben Sie Benutzern, eine Konfigurationsrichtlinie zu erstellen und zu verwalten

- Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen
- Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Security Hub Hub-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als

100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Security Hub CSPM-Konsole

Um auf die AWS Security Hub CSPM Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Security Hub CSPM-Ressourcen in Ihrem aufzulisten und anzuzeigen. AWS-Konto Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass diese Benutzer und Rollen die Security Hub CSPM-Konsole verwenden können, fügen Sie der Entität auch die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen, um diese Aktion auf der Konsole oder programmgesteuert mithilfe der API oder durchzuführen. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Erlauben Sie Benutzern, eine Konfigurationsrichtlinie zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Konfigurationsrichtlinien zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Diese Beispielrichtlinie ermöglicht es dem Benutzer auch, Richtlinienzuordnungen zu starten, zu beenden und anzuzeigen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer der delegierte Security Hub CSPM-Administrator für eine Organisation sein.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, die CSPM-Ergebnisse von Security Hub einzusehen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Security Hub CSPM-Automatisierungsregeln zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer ein Security Hub CSPM-Administrator sein. Um Berechtigungen einzuschränken — z. B. um einem Benutzer zu erlauben, nur Automatisierungsregeln einzusehen — können Sie die Berechtigungen zum Erstellen, Aktualisieren und Löschen entfernen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked Rollen für AWS Security Hub CSPM

AWS Security Hub CSPM verwendet eine dienstverknüpfte AWS Identity and Access Management (IAM) Rolle mit dem Namen. `AWSServiceRoleForSecurityHub` Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Security Hub CSPM verknüpft ist. Es ist von Security Hub CSPM vordefiniert und beinhaltet alle Berechtigungen, die Security Hub CSPM benötigt, um andere anzurufen AWS-Services und AWS Ressourcen in Ihrem Namen zu überwachen. Security Hub CSPM verwendet diese dienstbezogene Rolle in allen Bereichen, in AWS-Regionen denen Security Hub CSPM verfügbar ist.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Security Hub CSPM, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Security Hub CSPM definiert die Berechtigungen seiner dienstbezogenen Rolle, und sofern nicht anders definiert, kann nur Security Hub CSPM die Rolle übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und Sie können diese Berechtigungsrichtlinie keiner anderen IAM-Entität zuordnen.

Um die Details der dienstbezogenen Rolle zu überprüfen, können Sie die Security Hub CSPM-Konsole verwenden. Wählen Sie im Navigationsbereich unter Einstellungen die Option Allgemein aus. Wählen Sie dann im Abschnitt Dienstberechtigungen die Option Dienstberechtigungen anzeigen aus.

Sie können die dienstverknüpfte Rolle Security Hub CSPM erst löschen, nachdem Sie Security Hub CSPM in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dadurch werden Ihre Security Hub CSPM-Ressourcen geschützt, da Sie nicht versehentlich Zugriffsberechtigungen entfernen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Rollenspalte nach den Diensten, für die Ja steht. Service-linked Wählen Sie Ja mit einem Link aus, um die Dokumentation der dienstbezogenen Rollen für diesen Dienst zu lesen.

Themen

- Service-linked Rollenberechtigungen für Security Hub CSPM
- Eine serviceverknüpfte Rolle für Security Hub CSPM erstellen
- Eine serviceverknüpfte Rolle für Security Hub CSPM bearbeiten
- Löschen einer serviceverknüpften Rolle für Security Hub CSPM

Service-linked Rollenberechtigungen für Security Hub CSPM

Security Hub CSPM verwendet die benannte dienstverknüpfte Rolle. `AWSServiceRoleForSecurityHub` Es handelt sich um eine dienstbezogene Rolle, die für den Zugriff AWS Security Hub CSPM auf Ihre Ressourcen erforderlich ist. Diese dienstbezogene Rolle ermöglicht es Security Hub CSPM, Aufgaben wie das Empfangen von Ergebnissen von anderen auszuführen AWS-Services und die erforderliche AWS Config Infrastruktur für die Durchführung von Sicherheitsprüfungen für Kontrollen zu konfigurieren. Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHub` vertraut dem Service `securityhub.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHub` verwendet die verwaltete Richtlinie `AWSSecurityHubServiceRolePolicy`.

Sie müssen einer IAM-Identität (z. B. einer Rolle, Gruppe oder einem Benutzer) Berechtigungen erteilen, um eine dienstverknüpfte Rolle zu erstellen, zu bearbeiten oder zu löschen. Damit die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie für den Zugriff auf Security Hub CSPM verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Identität an.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Eine serviceverknüpfte Rolle für Security Hub CSPM erstellen

Die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle wird automatisch erstellt, wenn Sie Security Hub CSPM zum ersten Mal aktivieren oder wenn Sie Security Hub CSPM in einer Region aktivieren, in der Sie es zuvor nicht aktiviert haben. Sie können die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle auch manuell mithilfe der IAM-Konsole, der IAM-CLI oder der IAM-API erstellen. Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

> **Important**
>
> Die dienstverknüpfte Rolle, die für ein Security Hub CSPM-Administratorkonto erstellt wurde, gilt nicht für zugehörige Security Hub CSPM-Mitgliedskonten.

Eine serviceverknüpfte Rolle für Security Hub CSPM bearbeiten

Security Hub CSPM erlaubt es Ihnen nicht, die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Security Hub CSPM

Wenn Sie ein Feature oder einen Service nicht mehr benötigen, die bzw. der eine serviceverknüpfte Rolle erfordert, sollten Sie die Rolle löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird.

Wenn Sie Security Hub CSPM deaktivieren, löscht Security Hub CSPM die `AWSServiceRoleForSecurityHub` dienstverknüpfte Rolle nicht automatisch für Sie. Wenn Sie Security Hub CSPM erneut aktivieren, kann der Dienst die bestehende dienstverknüpfte Rolle wieder verwenden. Wenn Sie Security Hub CSPM nicht mehr verwenden müssen, können Sie die serviceverknüpfte Rolle manuell löschen.

> **Important**
>
> Bevor Sie die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle löschen, müssen Sie zunächst Security Hub CSPM in allen Regionen deaktivieren, in denen sie aktiviert ist. Weitere Informationen finden Sie unter Security Hub CSPM deaktivieren. Wenn Security Hub CSPM nicht deaktiviert ist, wenn Sie versuchen, die serviceverknüpfte Rolle zu löschen, schlägt der Löschvorgang fehl.

Um die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle zu löschen, können Sie die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Security Hub

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird. AWS AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSSecurityHubFullAccess

Sie können die `AWSSecurityHubFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Security Hub CSPM-Aktionen gewähren. Diese Richtlinie muss einem Prinzipal zugewiesen werden, bevor er Security Hub CSPM manuell für sein Konto aktiviert. Principals mit diesen Berechtigungen können beispielsweise den Status der Ergebnisse sowohl einsehen als auch aktualisieren. Sie können auch benutzerdefinierte Einblicke konfigurieren, Integrationen aktivieren sowie Standards und Kontrollen aktivieren und deaktivieren. Principals für ein Administratorkonto können auch Mitgliedskonten verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `securityhub`— Ermöglicht Principals vollen Zugriff auf alle Security Hub CSPM-Aktionen.
- `guardduty`— Ermöglicht Prinzipalen die vollständige Lebenszyklusverwaltung eines Melders, die Verwaltung der Organisation, die Verwaltung von Mitgliedskonten und die organisationsweite Konfiguration in Amazon. GuardDuty Dazu gehören API-Aktionen: GetDetector,,,, ListDetector, CreateDetector, UpdateDetector, DeleteDetector, EnableOrganizationAdminAccount. ListOrganizationAdminAccounts CreateMembers UpdateOrganizationConfiguration DescribeOrganizationConfiguration
- `iam`— Ermöglicht Prinzipalen, eine dienstbezogene Rolle für Security Hub CSPM und Security Hub zu erstellen und Rollen, Richtlinien und Richtlinienversionen abzurufen.
- `inspector`— Ermöglicht es Prinzipalen, Informationen über den Kontostatus abzurufen, sie zu aktivieren oder zu deaktivieren, die Administratorverwaltung zu delegieren und die Organisationskonfigurationsverwaltung in Amazon Inspector durchzuführen. Dazu gehören API-Aktionen: BatchGetAccountStatus, Aktivieren, Deaktivieren,,, EnableDelegatedAdminAccount, DisableDelegatedAdminAccount ListDelegatedAdminAccounts, UpdateOrganizationConfiguration. DescribeOrganizationConfiguration
- `pricing`— Ermöglicht Auftraggebern, eine Preisliste mit Produkten AWS-Services zu erhalten.

- `account`— Ermöglicht Prinzipalen das Abrufen von Informationen zu Kontoregionen, um die Regionsverwaltung in Security Hub zu unterstützen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSecurityHubReadOnlyAccess

Sie können die `AWSSecurityHubReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in Security Hub CSPM einzusehen. Principals, denen diese Richtlinie beigefügt ist, können keine Updates in Security Hub CSPM vornehmen. Principals mit diesen Berechtigungen können beispielsweise die mit ihrem Konto verknüpfte Ergebnisliste einsehen, den Status eines Fundes jedoch nicht ändern. Sie können die Ergebnisse von Insights einsehen, aber keine benutzerdefinierten Insights erstellen oder konfigurieren. Sie können keine Steuerungen oder Produktintegrationen konfigurieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `securityhub`— Ermöglicht Benutzern das Ausführen von Aktionen, bei denen eine Liste von Artikeln oder Details zu einem Artikel zurückgegeben wird. Dazu gehören API-Operationen, die mit `GetList`, oder beginnen`Describe`.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubReadOnlyAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSecurityHubOrganizationsAccess

Sie können die `AWSSecurityHubOrganizationsAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen zur Aktivierung und Verwaltung von Security Hub, Security Hub CSPM, Amazon GuardDuty und Amazon Inspector für eine Organisation in. AWS Organizations Die Berechtigungen für diese Richtlinie ermöglichen es dem Organisationsverwaltungskonto, das delegierte Administratorkonto für Security Hub, Security Hub CSPM, Amazon und Amazon GuardDuty Inspector zu bestimmen. Sie ermöglichen es dem delegierten Administratorkonto auch, Organisationskonten als Mitgliedskonten zu aktivieren.

Diese Richtlinie bietet nur Berechtigungen für AWS Organizations. Für das Organisationsverwaltungskonto und das delegierte Administratorkonto sind ebenfalls Berechtigungen für zugehörige Aktionen erforderlich. Diese Berechtigungen können mithilfe der `AWSSecurityHubFullAccess` verwalteten Richtlinie erteilt werden.

Das Erstellen oder Aktualisieren einer delegierten Administratorrichtlinie in einem Verwaltungskonto erfordert zusätzliche Berechtigungen, die in dieser Richtlinie nicht bereitgestellt werden. Um diese Aktionen durchzuführen, wird empfohlen, Berechtigungen für die AWSOrganizationsFullAccess Richtlinie hinzuzufügen `organizations:PutResourcePolicy` oder sie anzuhängen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `organizations:ListAccounts`— Ermöglicht Prinzipalen das Abrufen der Liste der Konten, die Teil einer Organisation sind.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisation.
- `organizations:ListRoots`— Ermöglicht Prinzipalen, das Stammverzeichnis einer Organisation aufzulisten.
- `organizations:ListDelegatedAdministrators`— Ermöglicht Prinzipalen, den delegierten Administrator einer Organisation aufzulisten.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Prinzipalen, diejenigen aufzulisten AWS-Services , die eine Organisation verwendet.
- `organizations:ListOrganizationalUnitsForParent`— Ermöglicht Prinzipalen, die untergeordneten Organisationseinheiten (OU) einer übergeordneten OU aufzulisten.
- `organizations:ListAccountsForParent`— Ermöglicht Prinzipalen, die untergeordneten Konten einer übergeordneten Organisationseinheit aufzulisten.
- `organizations:ListParents`— Führt die Stamm- oder Organisationseinheiten (OUs) auf, die der angegebenen untergeordneten Organisationseinheit oder dem angegebenen untergeordneten Konto als unmittelbare übergeordnete Einheit dienen.
- `organizations:DescribeAccount` – Ermöglicht Prinzipalen den Abruf von Informationen über ein Konto in der Organisation.
- `organizations:DescribeOrganizationalUnit`— Ermöglicht Prinzipalen das Abrufen von Informationen über eine Organisationseinheit in der Organisation.

- `organizations:ListPolicies`— Ruft die Liste aller Richtlinien in einer Organisation eines bestimmten Typs ab.
- `organizations:ListPoliciesForTarget`— Führt die Richtlinien auf, die direkt mit dem angegebenen Zielstamm, der Organisationseinheit (OU) oder dem angegebenen Konto verknüpft sind.
- `organizations:ListTargetsForPolicy`— Führt alle Stammverzeichnisse, Organisationseinheiten (OUs) und Konten auf, denen die angegebene Richtlinie zugeordnet ist.
- `organizations:EnableAWSServiceAccess`— Ermöglicht Prinzipalen, die Integration mit Organizations zu ermöglichen.
- `organizations:RegisterDelegatedAdministrator`— Ermöglicht es den Prinzipalen, das delegierte Administratorkonto festzulegen.
- `organizations:DeregisterDelegatedAdministrator`— Ermöglicht Prinzipalen, das delegierte Administratorkonto zu entfernen.
- `organizations:DescribePolicy`— Ruft Informationen zu einer Richtlinie ab.
- `organizations:DescribeEffectivePolicy`— Gibt den Inhalt der gültigen Richtlinie für den angegebenen Richtlinientyp und das angegebene Konto zurück.
- `organizations:CreatePolicy`— Erstellt eine Richtlinie eines bestimmten Typs, die Sie einem Stammkonto, einer Organisationseinheit (OU) oder einem einzelnen AWS Konto zuordnen können.
- `organizations:UpdatePolicy`— Aktualisiert eine bestehende Richtlinie mit einem neuen Namen, einer neuen Beschreibung oder einem neuen Inhalt.
- `organizations:DeletePolicy`— Löscht die angegebene Richtlinie aus Ihrer Organisation.
- `organizations:AttachPolicy`— Fügt eine Richtlinie einem Stammkonto, einer Organisationseinheit (OU) oder einem Einzelkonto hinzu.
- `organizations:DetachPolicy`— Trennt eine Richtlinie von einem Zielstamm, einer Organisationseinheit (OU) oder einem Zielkonto.
- `organizations:EnablePolicyType`— Aktiviert einen Richtlinientyp in einem Stamm.
- `organizations:DisablePolicyType`— Deaktiviert einen Organisationsrichtlinientyp in einem Stamm.
- `organizations:TagResource`— Fügt einer angegebenen Ressource ein oder mehrere Tags hinzu.
- `organizations:UntagResource`— Entfernt alle Tags mit den angegebenen Schlüsseln aus einer angegebenen Ressource.

- `organizations:ListTagsForResource`— Listet Tags auf, die an eine angegebene Ressource angehängt sind.
- `organizations:DescribeResourcePolicy`— Ruft Informationen über eine Ressourcenrichtlinie ab.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubOrganizationsAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSecurityHubServiceRolePolicy

Sie können `AWSSecurityHubServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Security Hub CSPM ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter the section called “Service-linked Rollen”.

Diese Richtlinie gewährt Administratorberechtigungen, die es der dienstbezogenen Rolle ermöglichen, Aufgaben wie die Ausführung von Sicherheitsprüfungen für Security Hub CSPM-Steuerelemente auszuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `cloudtrail`— Ruft Informationen über Wanderwege ab. CloudTrail
- `cloudwatch`— Rufen Sie aktuelle CloudWatch Alarme und Connector-Integritätskennzahlen ab.
- `logs`— Rufen Sie Metrikfilter für CloudWatch Protokolle ab.
- `sns`— Ruft die Liste der Abonnements für ein SNS-Thema ab.
- `config`— Ruft Informationen zu Konfigurationsrekordern, Ressourcen und AWS Config Regeln ab. Verwalten Sie die serviceverknüpften CSPM-Konfigurationsrekorder von Security Hub und die serviceverknüpften Konfigurationsrekorder von Drittanbietern. Erstellen und löschen Sie Regeln und führen Sie AWS Config Evaluierungen anhand der Regeln durch. Listet Konfigurationsrekorder auf und ruft Konnektorinformationen zur Unterstützung von Cloud-Integrationen von Drittanbietern ab.
- `iam`— Abrufen und Generieren von Berichten über Anmeldeinformationen für Konten und Erstellen der dienstverknüpften Rolle für. AWS Config
- `organizations`— Rufen Sie Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.

- `securityhub`— Rufen Sie Informationen darüber ab, wie der Security Hub CSPM-Dienst, die Standards und die Kontrollen konfiguriert sind.
- `tag`— Ruft Informationen über Ressourcen-Tags ab.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSSecurityHubServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Security Hub Hub-Updates für AWS Verwaltete Richtlinien

Die folgende Tabelle enthält Einzelheiten zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Security Hub und Security Hub CSPM, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Security Hub Hub-Dokumentverlaufsseite, um automatische Benachrichtigungen über Aktualisierungen der Richtlinien zu erhalten.

Änderungen	Beschreibung	Date
AWSSecurityHubServiceRolePolicy – Richtlinie aktualisieren	Security Hub CSPM hat die Richtlinie aktualisiert, um die Integration von Drittanbietern zu unterstützen. Das Update fügt die folgenden Berechtigungen hinzu: Konfigurationsrekorder von Drittanbietern verwalten, Konfigurationsrekorder auflisten, Connectorinformationen abrufen und Connector-Integritätsmetriken abrufen.	30. Juni 2026
AWSSecurityHubServiceRolePolicy – Richtlinie aktualisieren	Security Hub CSPM hat die Richtlinie aktualisiert, um Berechtigungen zur Verwaltung von serviceverknüpften Security Hub CSPM-Konfigurationsrekordern und zur	29. April 2026

Änderungen	Beschreibung	Date
	Erstellung der dienstbez ogenen Rolle hinzuzufügen. AWS Config	
AWSSecurityHubOrga nizationsAccess – Richtlinie aktualisieren	Security Hub hat die Richtlini e aktualisiert, um Berechtig ungen zur Beschreibung von Ressourcenrichtlin ien zur Unterstützung von Security Hub Hub-Funktionen hinzuzufügen. Security Hub befindet sich in der Vorschauv ersion und kann sich ändern.	12. November 2025
AWSSecurityHubFullAccess – Richtlinie aktualisieren	Security Hub hat die Richtlini e aktualisiert und Funktione n zur Verwaltung GuardDuty , Amazon Inspector und Kontoverwaltung hinzugefü gt, um die Funktionen von Security Hub zu unterstützen. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	17. November 2025
AWSSecurityHubOrga nizationsAccess – Aktualisi erung auf eine bestehende Richtlinie	Security Hub hat der Richtlini e neue Berechtigungen hinzugefügt. Die Berechtig ungen ermöglichen es der Organisationsleitung, Security Hub und Security Hub CSPM für eine Organisation zu aktivieren und zu verwalten.	17. Juni 2025

Änderungen	Beschreibung	Date
AWSSecurityHubFullAccess – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, eine dienstbezogene Rolle für Security Hub zu erstellen.	17. Juni 2025
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um Preisdetails für AWS-Services und Produkte zu erhalten.	24. April 2024
AWSSecurityHubReadOnlyAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat diese verwaltete Richtlinie aktualisiert, indem ein `Sid` Feld hinzugefügt wurde.	22. Februar 2024
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, sodass festgestellt werden kann, ob Amazon GuardDuty und Amazon Inspector in einem Konto aktiviert sind. Dies hilft Kunden dabei, sicherheitsrelevante Informationen aus mehreren zusammenzuführen. AWS-Services	16. November 2023

Änderungen	Beschreibung	Date
AWSSecurityHubOrganizationsAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um zusätzliche Berechtigungen für den schreibgeschützten Zugriff auf delegierte Administratorfunktionen zu AWS Organizations gewähren. Dazu gehören Details wie das Stammverzeichnis, die Organisationseinheiten (OUs), die Konten, die Organisationsstruktur und der Servicezugriff.	16. November 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die `UpdateSecurityControl` Berechtigungen `BatchGetSecurityControls` `DisassociateFromAdministratorAccount` , und zum Lesen und Aktualisieren anpassbarer Sicherheitskontrolleigenschaften hinzugefügt.	26. November 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die `tag:GetResources` Erlaubnis hinzugefügt, Ressourcen-Tags zu lesen, die sich auf Ergebnisse beziehen.	7. November 2023

Änderungen	Beschreibung	Date
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die `BatchGetStandardsControlAssociations` Erlaubnis hinzugefügt, Informationen über den Aktivierungsstatus einer Steuerung in einem Standard abzurufen.	27. September 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat neue Berechtigungen zum Abrufen von AWS Organizations Daten sowie zum Lesen und Aktualisieren von Security Hub CSPM-Konfigurationen, einschließlich Standards und Kontrollen, hinzugefügt.	20. September 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die bestehende `config:DescribeConfigRuleEvaluationStatus` Berechtigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die `config:DescribeConfigRuleEvaluationStatus` Erlaubnis wird jetzt auf alle Ressourcen angewendet.	17. März 2023

Änderungen	Beschreibung	Date
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die bestehende `config:PutEvaluations` Berechtigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die `config:PutEvaluations` Erlaubnis wird jetzt auf alle Ressourcen angewendet.	14. Juli 2021
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat eine neue Berechtigung hinzugefügt, die es der serviceverknüpften Rolle ermöglicht, Bewertungsergebnisse zu liefern. AWS Config	29. Juni 2021
AWSSecurityHubServiceRolePolicy— Zur Liste der verwalteten Richtlinien hinzugefügt	Es wurden Informationen zur verwalteten Richtlinie hinzugefügt AWSSecurityHubServiceRolePolicy, die von der serviceverknüpften Rolle Security Hub CSPM verwendet wird.	11. Juni 2021
AWSSecurityHubOrganizationsAccess— Neue Richtlinie	Security Hub CSPM hat eine neue Richtlinie hinzugefügt, die Berechtigungen gewährt, die für die Security Hub CSPM-Integration mit Organizations erforderlich sind.	15. März 2021

Änderungen	Beschreibung	Date
Security Hub CSPM hat begonnen, Änderungen zu verfolgen	Security Hub CSPM begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	15. März 2021

Fehlerbehebung AWS Security Hub CSPM Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Security Hub CSPM und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Security Hub CSPM durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte programmatischen Zugriff auf Security Hub CSPM
- Ich bin Administrator und möchte anderen den Zugriff auf Security Hub CSPM ermöglichen
- Ich möchte Personen außerhalb meines AWS-Konto um auf meine Security Hub CSPM-Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Security Hub CSPM durchzuführen

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einem anzuzeigen, *`widget`* aber nicht über die `securityhub:`*`GetWidget`* entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `securityhub:`*`GetWidget`* zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Security Hub übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Security Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte programmatischen Zugriff auf Security Hub CSPM

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS-Managementkonsole Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldedaten als temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	CLI, AWS SDKs oder APIs zu signieren. AWS	• Informationen zu den AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzh andbuch für AWS SDKs und Tools.
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisung en für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benut zeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldein formationen im Referenzh andbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltun g von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benut zerhandbuch.

Ich bin Administrator und möchte anderen den Zugriff auf Security Hub CSPM ermöglichen

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in: AWS IAM Identity Center

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS-Konto um auf meine Security Hub CSPM-Ressourcen zuzugreifen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Security Hub diese Funktionen unterstützt, finden Sie unterSo funktioniert Security Hub mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.

- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsprüfung für AWS Security Hub CSPM

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeformular nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für AWS (erweiterte) Funktionen registrieren oder erweiterte Funktionen für Ihre Umgebung aktivieren. AWS

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz in AWS Security Hub

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Security Hub CSPM

Als verwalteter Dienst AWS Security Hub CSPM ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Security Hub CSPM zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

AWS Security Hub CSPM und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Security Hub CSPM durch die Erstellung eines Schnittstellen-VPC-Endpunkts herstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Security Hub CSPM-APIs zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit den Security Hub CSPM-APIs zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und Security Hub CSPM verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon Virtual Private Cloud Guide.

Überlegungen zu Security Hub CSPM VPC-Endpunkten

Bevor Sie einen VPC-Schnittstellen-Endpunkt für Security Hub CSPM einrichten, stellen Sie sicher, dass Sie die Voraussetzungen und andere Informationen im Amazon Virtual Private Cloud Guide lesen.

Security Hub CSPM unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

Einen VPC-Schnittstellen-Endpunkt für Security Hub CSPM erstellen

Sie können einen VPC-Endpunkt für den Security Hub CSPM-Service entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im Amazon Virtual Private Cloud Cloud-Handbuch.

Erstellen Sie einen VPC-Endpunkt für Security Hub CSPM mit dem folgenden Dienstnamen:

`com.amazonaws.region.securityhub`

Wo *region* ist der Regionalcode für den zutreffenden. AWS-Region

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Security Hub CSPM stellen, indem Sie dessen Standard-DNS-Namen für die Region verwenden, z. B. `securityhub.us-east-1.amazonaws.com` für die Region USA Ost (Nord-Virginia).

VPC-Endpunktrichtlinie für Security Hub CSPM erstellen

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Security Hub CSPM steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon Virtual Private Cloud Cloud-Handbuch.

Beispiel: VPC-Endpunktrichtlinie für Security Hub CSPM-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Security Hub CSPM. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Security Hub CSPM-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
```

```
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Gemeinsam genutzte Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen geteilt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden. Informationen zur VPC-Sharing finden Sie unter Teilen Sie Ihre VPC-Subnetze mit anderen Konten im Amazon Virtual Private Cloud Cloud-Leitfaden.

Security Hub Hub-API-Aufrufe protokollieren mit CloudTrail

AWSSecurity Hub CSPM ist in einen Dienst integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Security Hub CSPM ausgeführt wurden. CloudTrail erfasst API-Aufrufe für Security Hub CSPM als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Hub CSPM-Konsole und Code-Aufrufe an die Security Hub CSPM-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Security Hub CSPM. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der CloudTrail gesammelten Informationen können Sie die Anfrage, die an Security Hub CSPM gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrailBenutzerhandbuch.

Security Hub CSPM-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWS-Konto, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in Security Hub CSPM auftreten, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem Konto, einschließlich Ereignissen für Security Hub CSPM, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Security Hub CSPM unterstützt die Protokollierung aller Security Hub CSPM-API-Aktionen als Ereignisse in Protokollen. CloudTrail Eine Liste der Security Hub CSPM-Operationen finden Sie in der Security Hub CSPM API-Referenz.

Wenn Aktivitäten für die folgenden Aktionen protokolliert werden CloudTrail, ist der Wert für `responseElements` auf gesetzt. `null` Dadurch wird sichergestellt, dass vertrauliche Informationen nicht in den CloudTrail Protokollen enthalten sind.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde

- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Beispiel: Security Hub CSPM-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateInsight` Aktion demonstriert. In diesem Beispiel wird ein Insight mit dem Namen `Test Insight` erstellt. Das `ResourceId` Attribut ist als Gruppieren nach Aggregator angegeben, und es wurden keine optionalen Filter für diesen Einblick angegeben. Weitere Informationen über Funde sind unter Einblicke in Security Hub CSPM anzeigen verfügbar.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
```

```
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Kennzeichnen von Security Hub Hub-Ressourcen

Ein Tag ist eine optionale Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Typen von AWS Security Hub CSPM-Ressourcen. Tags können Ihnen dabei helfen, Ressourcen auf verschiedene Arten zu identifizieren, zu kategorisieren und zu verwalten (z. B. nach Zweck, Besitzer, Umgebung oder anderen Kriterien). Mithilfe von Tags können Sie beispielsweise zwischen Ressourcen unterscheiden, Ressourcen identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen, oder Kosten zuordnen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Automatisierungsregeln
- Konfigurationsrichtlinien
- Hub-Ressource

Grundlagen des Kennzeichnens

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Beides können Sie definieren. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Wenn Sie beispielsweise unterschiedliche Automatisierungsregeln für verschiedene Umgebungen erstellen (einen Satz von Automatisierungsregeln für Testkonten und einen anderen für Produktionskonten), können Sie diesen Regeln einen `Environment` Tagschlüssel zuweisen. Der zugehörige Tagwert kann `Test` für die Regeln gelten, die Testkonten zugeordnet sind, und `Prod` für die Regeln, die Produktionskonten und Organisationseinheiten zugeordnet sind.

Beachten Sie bei der Definition und Zuweisung von Tags zu AWS Security Hub CSPM-Ressourcen Folgendes:

- Jede Ressource kann maximal 50 Tags haben.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein und er kann nur einen Tag-Wert haben.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Als bewährte Methode empfehlen wir Ihnen, eine Strategie zur Großschreibung von Tags zu definieren und diese Strategie in allen Ressourcen einheitlich umzusetzen.

- Ein Tag-Schlüssel kann maximal 128 UTF-8 Zeichen lang sein. Ein Tagwert kann maximal 256 UTF-8 Zeichen enthalten. Bei den Zeichen kann es sich um Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole handeln: _.:/= + - @
- Das `aws:` Präfix ist für die Verwendung durch reserviertAWS. Sie können es nicht in Tag-Schlüsseln oder -Werten verwenden, die Sie definieren. Außerdem können Sie Tag-Schlüssel oder -Werte, die dieses Präfix verwenden, nicht ändern oder entfernen. Tags mit diesem Präfix werden beim Kontingent von 50 Tags pro Ressource nicht eingerechnet.
- Alle Tags, die Sie zuweisen, sind nur für Sie AWS-Konto und nur in dem verfügbar, AWS-Region in dem Sie sie zuweisen.
- Wenn Sie einer Ressource mithilfe von Security Hub CSPM Tags zuweisen, werden die Tags nur auf die Ressource angewendet, die direkt im Security Hub CSPM im entsprechenden Verzeichnis gespeichert ist. AWS-Region Sie gelten nicht für zugehörige, unterstützende Ressourcen, die Security Hub CSPM in anderen Bereichen für Sie erstellt, verwendet oder verwaltet. AWS-Services Wenn Sie beispielsweise einer Automatisierungsregel, die Ergebnisse im Zusammenhang mit Amazon Simple Storage Service (Amazon S3) aktualisiert, Tags zuweisen, werden die Tags nur auf Ihre Automatisierungsregel in Security Hub CSPM für die angegebene Region angewendet. Sie werden nicht auf Ihre S3-Buckets angewendet. Um auch einer zugehörigen Ressource Tags zuzuweisen, können Sie AWS -Ressourcengruppen oder das verwenden, in dem AWS-Service die Ressource gespeichert ist, z. B. Amazon S3 für einen S3-Bucket. Das Zuweisen von Tags zu zugehörigen Ressourcen kann Ihnen dabei helfen, unterstützende Ressourcen für Ihre Security Hub CSPM-Ressourcen zu identifizieren.
- Wenn Sie eine Ressource löschen, werden alle Tags, die der Ressource zugewiesen sind, ebenfalls gelöscht.

> **Important**
>
> Speichern Sie keine vertraulichen oder anderen sensiblen Daten in Tags. Auf Tags kann von vielen aus zugegriffen werdenAWS-Services, darunterAWS Fakturierung und Kostenmanagement. Sie sind nicht dafür vorgesehen, für sensible Daten verwendet zu werden.

Um Tags für Security Hub CSPM-Ressourcen hinzuzufügen und zu verwalten, können Sie die Security Hub CSPM-Konsole, die Security Hub CSPM API oder die Tagging API verwenden. AWS -Ressourcengruppen Mit Security Hub CSPM können Sie einer Ressource Tags hinzufügen, wenn

Sie die Ressource erstellen. Sie können auch Tags für einzelne vorhandene Ressourcen hinzufügen und verwalten. Mit Resource Groups können Sie Tags für mehrere bestehende Ressourcen, einschließlich Security Hub CSPMAWS-Services, in großen Mengen hinzufügen und verwalten.

Weitere Tipps und bewährte Methoden zur Kennzeichnung finden Sie unter Tagging Your AWS Resources User Guide im Tagging Resources User Guide. AWS

Verwenden von Tags in IAM-Richtlinien

Nachdem Sie mit dem Taggen von Ressourcen begonnen haben, können Sie tagbasierte Berechtigungen auf Ressourcenebene in (IAM-) Richtlinien definieren. AWS Identity and Access Management Durch die Verwendung von Tags auf diese Weise können Sie detailliert steuern, welche Benutzer und Rollen in Ihrem Unternehmen die Berechtigung AWS-Konto haben, Ressourcen zu erstellen und zu taggen, und welche Benutzer und Rollen generell die Berechtigung haben, Tags hinzuzufügen, zu bearbeiten und zu entfernen. Um den Zugriff anhand von Tags zu steuern, können Sie im Element Condition der IAM-Richtlinien Tag-bezogene Bedingungsschlüssel verwenden.

Sie können beispielsweise eine IAM-Richtlinie erstellen, die einem Benutzer vollen Zugriff auf alle AWS Security Hub CSPM-Ressourcen gewährt, wenn das `Owner` Tag für die Ressource seinen Benutzernamen angibt:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Wenn Sie Tag-basierte Berechtigungen auf Ressourcenebene definieren, werden die Berechtigungen sofort wirksam. Dies bedeutet, dass Ihre Ressourcen besser geschützt sind, sobald sie erstellt wurden, und Sie schnell damit beginnen können, die Verwendung von Tags für neue Ressourcen zu erzwingen. Mithilfe von Berechtigungen auf Ressourcenebene können Sie auch steuern, welche Tag-Schlüssel und -Werte können mit neuen und vorhandenen Ressourcen verknüpft werden können. Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags im IAM-Benutzerhandbuch.

Hinzufügen von Tags zu Security Hub CSPM-Ressourcen

Ein Tag ist eine Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Typen von AWS Security Hub CSPM-Ressourcen. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Automatisierungsregeln
- Konfigurationsrichtlinien
- Hub-Ressource

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel. Weitere Informationen zu Tag-Optionen und Anforderungen finden Sie unterGrundlagen des Kennzeichnens.

Um einer Security Hub CSPM-Ressource Tags hinzuzufügen, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Die Konsole unterstützt jedoch nicht das Hinzufügen von Tags zur Ressource. Hub

Nachdem Sie Tags hinzugefügt haben, können Sie das Tag bearbeiten und den Tag-Schlüssel oder den Tag-Wert ändern.

Verwenden Sie die Tagging-Operationen der Tagging-API, um Tags für mehrere Security Hub CSPM-Ressourcen gleichzeitig hinzuzufügen oder zu bearbeiten. AWS -Ressourcengruppen

> **Important**
>
> Das Hinzufügen von Tags zu einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einer Ressource ein Tag hinzufügen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

So fügen Sie einer Security Hub CSPM-Ressource (Konsole) Tags hinzu

Wenn Sie eine Automatisierungsregel oder eine Konfigurationsrichtlinie erstellen, bietet die Security Hub CSPM-Konsole Optionen zum Hinzufügen von Tags. Sie können den Tag-Schlüssel und den Tag-Wert im Abschnitt Tags angeben.

Security Hub CSPM API

So fügen Sie einer Security Hub CSPM-Ressource (API) Tags hinzu

Um eine Ressource zu erstellen und ihr programmgesteuert ein oder mehrere Tags hinzuzufügen, verwenden Sie die entsprechende Operation für den Ressourcentyp, den Sie erstellen möchten:

- Um eine Konfigurationsrichtlinie zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die CreateConfigurationPolicyAPI auf oder führen Sie, falls Sie die verwendenAWS CLI, den Befehl create-configuration-policy aus.
- Um eine Automatisierungsregel zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die CreateAutomationRuleAPI auf oder führen Sie, falls Sie die verwenden, den AWS CLI Befehl create-automation-rule aus.
- Um Security Hub CSPM zu aktivieren und Ihrer Hub Ressource ein oder mehrere Tags hinzuzufügen, rufen Sie die EnableSecurityHubAPI auf oder führen Sie, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, den Befehl enable-security-hub aus.

Verwenden Sie in Ihrer Anfrage den `tags` Parameter, um den Tag-Schlüssel und den optionalen Tag-Wert für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Der `tags`

Parameter gibt ein Array von Objekten an. Jedes Objekt gibt einen Tag-Schlüssel und den zugehörigen Tag-Wert an.

Um einer vorhandenen Ressource ein oder mehrere Tags hinzuzufügen, verwenden Sie den TagResourceBetrieb der Security Hub CSPM-API oder, falls Sie den verwendenAWS CLI, führen Sie den Befehl tag-resource aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, der Sie ein Tag hinzufügen möchten. Verwenden Sie den `tags` Parameter, um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes hinzuzufügende Tag anzugeben. Der `tags` Parameter gibt ein Array von Objekten an, ein Objekt für jeden Tag-Schlüssel und den zugehörigen Tag-Wert.

Der folgende AWS CLI Befehl fügt beispielsweise der angegebenen Konfigurationsrichtlinie einen `Prod` Tag-Schlüssel mit einem Tag-Wert hinzu. `Environment` Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

Beispiel für einen CLI-Befehl:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Wobei Folgendes gilt:

- `resource-arn`gibt den ARN der Konfigurationsrichtlinie an, zu der ein Tag hinzugefügt werden soll.
- *`Environment`*ist der Tag-Schlüssel des Tags, das der Regel hinzugefügt werden soll.
- *`Prod`*ist der Tag-Wert für den angegebenen Tag-Schlüssel (*`Environment`*).

Im folgenden Beispiel fügt der Befehl der Konfigurationsrichtlinie mehrere Tags hinzu.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Für jedes Objekt in einem `tags` Array sind `key` sowohl die `value` Argumente als auch erforderlich. Der Wert für das `value` Argument kann jedoch eine leere Zeichenfolge sein. Wenn

Sie einem Tag-Schlüssel keinen Tag-Wert zuordnen möchten, geben Sie keinen Wert für das `value` Argument an. Mit dem folgenden Befehl wird beispielsweise ein `Owner` Tag-Schlüssel ohne zugehörigen Tag-Wert hinzugefügt:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Wenn ein Tagging-Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags für Security Hub CSPM-Ressourcen bearbeiten

Wenn sich Ihre Umgebung oder Anforderungen im Laufe der Zeit ändern, können Sie vorhandene Tags für Ihre AWS Security Hub CSPM-Ressourcen auswerten und die Tags nach Bedarf ändern. Ein Tag ist eine Bezeichnung, die Sie definieren und einer oder mehreren AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Macie-Ressourcen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Tags können Ihnen dabei helfen, Ressourcen auf verschiedene Arten zu identifizieren, zu kategorisieren und zu verwalten (z. B. nach Zweck, Besitzer, Umgebung oder anderen Kriterien). Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Automatisierungsregeln
- Konfigurationsrichtlinien
- Hub-Ressource

Um Tag-Schlüssel oder Tag-Werte für eine Security Hub CSPM-Ressource zu bearbeiten, können Sie die Security Hub CSPM-API verwenden. Die Security Hub CSPM-Konsole unterstützt derzeit keine Tag-Bearbeitung.

> **Important**
>
> Das Bearbeiten von Tags für eine Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag für eine Ressource bearbeiten, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Security Hub CSPM API

So bearbeiten Sie Tags für eine Security Hub CSPM-Ressource (API)

Wenn Sie ein Tag für eine Ressource programmgesteuert bearbeiten, überschreiben Sie das vorhandene Tag mit neuen Werten. Daher hängt die beste Methode zum Bearbeiten eines Tags davon ab, ob Sie einen Tag-Schlüssel, einen Tag-Wert oder beides bearbeiten möchten. Um einen Tag-Schlüssel zu bearbeiten, entfernen Sie das aktuelle Tag und fügen Sie ein neues Tag hinzu.

Um nur den Tag-Wert zu bearbeiten oder zu entfernen, der einem Tag-Schlüssel zugeordnet ist, überschreiben Sie den vorhandenen Wert mithilfe TagResourceder Security Hub CSPM-API. Wenn Sie den verwenden, führen Sie den Befehl AWS CLI tag-resource aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, deren Tag-Wert Sie bearbeiten oder entfernen möchten.

Um einen Tag-Wert zu bearbeiten, verwenden Sie den `tags` Parameter, um den Tag-Schlüssel anzugeben, dessen Tag-Wert Sie ändern möchten. Sie sollten auch den neuen Tag-Wert für den Schlüssel angeben. Mit dem folgenden AWS CLI Befehl wird beispielsweise der Tag-Wert `Test` für `Prod` den `Environment` Tag-Schlüssel, der der angegebenen Automatisierungsregel zugewiesen ist, von auf geändert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Wobei Folgendes gilt:

- `resource-arn`gibt den ARN der Konfigurationsrichtlinie an.
- *`Environment`*ist der Tag-Schlüssel, der dem zu ändernden Tag-Wert zugeordnet ist.
- *`Test`*ist der neue Tag-Wert für den angegebenen Tag-Schlüssel (*`Environment`*).

Um einen Tag-Wert aus einem Tag-Schlüssel zu entfernen, geben Sie im `tags` Parameter keinen Wert für das `value` Argument des Schlüssels an. Beispiel:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags für Security Hub CSPM-Ressourcen überprüfen

Nachdem Sie Tags für AWS Security Hub CSPM-Ressourcen hinzugefügt oder bearbeitet haben, können Sie sehen, über welche Tag-Schlüssel und Tag-Werte eine Ressource derzeit verfügt. Ein Tag ist eine Bezeichnung, die Sie definieren und einer oder mehreren AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Macie-Ressourcen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Tags können Ihnen dabei helfen, Ressourcen auf verschiedene Arten zu identifizieren, zu kategorisieren und zu verwalten (z. B. nach Zweck, Besitzer, Umgebung oder anderen Kriterien). Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Automatisierungsregeln

- Konfigurationsrichtlinien
- Hub-Ressource

Sie können die Tags für eine Security Hub CSPM-Automatisierungsregel oder eine Konfigurationsrichtlinie überprüfen, indem Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Die Konsole unterstützt die Überprüfung von Tags für die Ressource nicht. Hub Programmgesteuert können Sie Tags für jede Ressource überprüfen.

Verwenden Sie die Tagging-Operationen der Tagging-API, um Tags für mehrere Security Hub CSPM-Ressourcen gleichzeitig zu überprüfen. AWS -Ressourcengruppen

Console

So überprüfen Sie Tags für eine Security Hub CSPM-Ressource (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub CSPM-Konsole unter. https://console.aws.amazon.com/securityhub/
2. Gehen Sie je nach Art der Ressource, der Sie ein Tag hinzufügen möchten, wie folgt vor:
   - Um die Tags für eine Automatisierungsregel zu überprüfen, wählen Sie im Navigationsbereich Automatisierungen aus. Wählen Sie dann eine Automatisierungsregel aus.
   - Um die Tags für eine Konfigurationsrichtlinie zu überprüfen, wählen Sie im Navigationsbereich Konfiguration aus. Wählen Sie dann auf der Registerkarte Richtlinien die Option neben einer Konfigurationsrichtlinie aus. Es wird ein Seitenbereich geöffnet, in dem die Anzahl der der Richtlinie zugewiesenen Tags angezeigt wird. Sie können den Tags-Header erweitern, um die Tag-Schlüssel und Tag-Werte zu sehen.

Im Abschnitt „Tags“ werden alle Tags aufgeführt, die der Ressource derzeit zugewiesen sind.

Security Hub CSPM API

Um Tags für eine Security Hub CSPM-Ressource (API) zu überprüfen

Rufen Sie die API auf, um die Tags für eine bestehende Ressource abzurufen und zu überprüfen. ListTagsForResource Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben.

Wenn Sie den verwendenAWS CLI, führen Sie den Befehl list-tags-for-resource aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an. Beispiel:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM ein Array zurück. `tags` Jedes Objekt im Array spezifiziert ein Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert), das der Ressource aktuell zugewiesen ist. Beispiel:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Wobei `Environment``CostCenter`, und `Owner` die Tag-Schlüssel sind, die der Ressource zugewiesen sind. `Prod`ist der Tag-Wert, der dem `Environment` Tag-Schlüssel zugeordnet ist. `12345`ist der Tag-Wert, der dem `CostCenter` Tag-Schlüssel zugeordnet ist. Dem `Owner` Tag-Schlüssel ist kein Tag-Wert zugeordnet.

Um eine Liste aller Security Hub CSPM-Ressourcen mit Tags und aller Tags, die jeder dieser Ressourcen zugewiesen sind, abzurufen, verwenden Sie den GetResourcesBetrieb der AWS -Ressourcengruppen Tagging-API. Setzen Sie in Ihrer Anfrage den Wert für den Parameter auf`ResourceTypeFilters`. `securityhub` Führen Sie dazu mit dem den AWS CLI Befehl get-resources aus und setzen Sie den Wert für den `resource-type-filters` Parameter auf`securityhub`. Beispiel:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Wenn der Vorgang erfolgreich ist, gibt Resource Groups ein `ResourceTagMappingList` Array zurück. Das Array enthält ein Objekt für jede Security Hub-CSPM-Ressource, die über Tags verfügt. Jedes Objekt spezifiziert den ARN einer Security Hub-CSPM-Ressource sowie die Tag-Schlüssel und -Werte, die der Ressource zugewiesen sind.

Tags aus den CSPM-Ressourcen von Security Hub entfernen

Wenn Sie einer AWS Security Hub CSPM-Ressource Tags hinzufügen, können Sie anschließend eines oder mehrere davon entfernen. Ein Tag ist eine Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Security Hub CSPM-Ressourcen. Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen, bearbeiten und entfernen: Automatisierungsregeln, Konfigurationsrichtlinien und die Hub Ressource.

Um Tags aus einer einzelnen AWS Security Hub CSPM-Ressource zu entfernen, können Sie die Security Hub CSPM-API verwenden. Die Security Hub CSPM-Konsole unterstützt derzeit das Entfernen von Tags nicht.

Um Tags aus mehreren Security Hub CSPM-Ressourcen gleichzeitig zu entfernen, verwenden Sie die Tagging-Operationen der AWS -Ressourcengruppen Tagging-API.

> **Important**
>
> Das Entfernen von Tags aus einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag entfernen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die das Tag möglicherweise zur Steuerung des Zugriffs auf Ressourcen verwenden.

Security Hub CSPM API

So entfernen Sie Tags aus einer Security Hub CSPM-Ressource (API)

Um ein oder mehrere Tags programmgesteuert aus einer Ressource zu entfernen, verwenden Sie den UntagResourceBetrieb der Security Hub CSPM-API. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben, aus der ein Tag entfernt werden soll. Verwenden Sie den `tagKeys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Um mehrere Tags zu entfernen, hängen Sie den `tagKeys` Parameter und das Argument für jedes zu entfernende Tag an, getrennt durch

ein Und-Zeichen (&) — zum Beispiel. `tagKeys=key1&tagKeys=key2` Um nur einen bestimmten Tag-Wert (keinen Tag-Schlüssel) aus einer Ressource zu entfernen, bearbeiten Sie das Tag, anstatt das Tag zu entfernen.

Wenn Sie den verwendenAWS CLI, führen Sie den Befehl untag-resource aus, um ein oder mehrere Tags aus einer Ressource zu entfernen. Geben Sie für den `resource-arn` Parameter den ARN der Ressource an, aus der ein Tag entfernt werden soll. Verwenden Sie den `tag-keys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Mit dem folgenden Befehl wird beispielsweise das `Environment` Tag (sowohl der Tag-Schlüssel als auch der Tag-Wert) aus der angegebenen Konfigurationsrichtlinie entfernt:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Where `resource-arn` gibt den ARN der Konfigurationsrichtlinie an, aus der ein Tag entfernt werden soll, und *`Environment`* ist der Tag-Schlüssel des Tags, aus dem entfernt werden soll.

Um mehrere Tags aus einer Ressource zu entfernen, fügen Sie jeden zusätzlichen Tag-Schlüssel als Argument für den `tag-keys` Parameter hinzu. Beispiel:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Kontingente für Security Hub

Ihr AWS-Konto hat für jedes Kontingent bestimmte Standardkontingente, früher als Limits bezeichnet. AWS-Service Diese Kontingente sind die maximale Anzahl von Serviceressourcen oder Vorgängen für Ihr Konto. Dieses Thema enthält Links zu den Kontingenten, die für AWS Security Hub Hub-Ressourcen und -Vorgänge für Ihr Konto gelten. Sofern nicht anders angegeben, gilt jedes Kontingent jeweils für Ihr KontoAWS-Region.

Einige Kontingente können erhöht werden, andere dagegen nicht. Verwenden Sie die Service Quotas-Konsole, um eine Erhöhung eines Kontingents anzufordern. Informationen dazu, wie Sie eine Erhöhung beantragen können, finden Sie unter Eine Erhöhung des Kontingents beantragen im Benutzerhandbuch zu Service Quotas. Wenn ein Kontingent in der Service-Kontingents-Konsole nicht verfügbar ist, verwenden Sie das Formular zur Erhöhung des Servicelimits auf derAWS Support Center Console, um eine Erhöhung des Kontingents zu beantragen.

Maximale Kontingente

Eine Liste der Kontingente, die für AWS Security Hub Hub-Ressourcen gelten, finden Sie unter AWSSecurity Hub Hub-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Ratenkontingente

Eine Liste der Kontingente, die für AWS Security Hub Hub-API-Operationen gelten, finden Sie in der AWSSecurity Hub Hub-API-Referenz.

Wenn Sie die regionsübergreifende Aggregation in Security Hub CSPM einrichten, erfolgt ein einziger Aufruf `BatchImportFindings` und `BatchUpdateFindings` wirkt sich auf verknüpfte Regionen und die Aggregationsregion aus. Der `GetFindings` Vorgang ruft Ergebnisse aus verknüpften Regionen und der Aggregationsregion ab. Die `UpdateStandardsControl` Operationen `BatchEnableStandards` und sind es jedoch. Region-specific

Dokumentenhistorie für die AWS Security Hub Benutzer-Leitfaden

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von AWS Security Hub und Security Hub CSPM beschrieben. Bei Versionen neuer Security Hub CSPM-Steuerelemente gibt das Datum an, ab wann die Steuerelemente im unterstützten Bereich verfügbar sind. AWS-Regionen Es kann 1-2 Wochen dauern, bis die Kontrollen in allen unterstützten Regionen verfügbar sind. Einzelheiten zu wesentlichen Änderungen an bestehenden Kontrollen finden Sie unter. Änderungsprotokoll für Security Hub CSPM-Steuerelemente

Um Benachrichtigungen über Updates des AWS Security Hub Hub-Benutzerhandbuchs zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Neuer Sicherheitsstandard	Security Hub CSPM hat den Standard CRI Profile v2.2 veröffentlicht. Dieser Standard entspricht dem CRI Profile, einem vom Cyber Risk Institute (CRI) entwickelten Cybersicherheits-Framework, das die Cybersicherheits- und regulatorischen Erwartungen für den Finanzdienstleistungssektor harmonisiert.	14. Oktober 2026
Automatisierungsregeln können die Wichtigkeit von Ressourcen aktualisieren	Mit den Security Hub Hub-Automatisierungsregeln können jetzt neben der Aktualisierung von Suchdetails und der Erstellung von Tickets auch die Wichtigkeit von Ressourcen (Ressourcenregeln) aktualisiert werden. Die Festlegung der Ressource	1. Oktober 2026

	npriorität hilft Ihnen dabei, Problembehebungen danach zu priorisieren, wie wichtig die betroffenen Ressourcen für Ihr Unternehmen sind.	
Sanierungspläne	Es wurden Abhilfepläne hinzugefügt, in denen zusammengehörige Expositionsfeststellungen nach der Grundursache gruppiert werden, sodass mit einer Lösung der Schweregrad mehrerer Risiken behoben oder verringert werden kann. Weitere Informationen finden Sie unter Behebungspläne in AWS Security Hub.	30. September 2026
Die Informationen zu den Ergebnissen des Netzwerkscans wurden aktualisiert	Es wurden Informationen zu informativen Ergebnissen hinzugefügt, die beim Netzwerkscannen generiert werden.	3. September 2026
Die Liste der Netzwerkscanning-Ports wurde aktualisiert	Es wurde eine Liste der Ports hinzugefügt, die derzeit von Netzwerkscans unterstützt werden.	18. August 2026

Die Sicherheitskontrollen wurden aktualisiert	Security Hub CSPM hat die EFS.6Kontrolle aus dem Standard AWS Foundational Security Best Practices (FSBP) entfernt. Dieses Steuerelement ist weiterhin in den Standards NIST SP 800-53 Rev. 5, NIST SP 800-171 Revision 2 und PCI DSS v4.0.1 verfügbar.	3. August 2026
Dokumentation zur erweiterten Aktivierung von Security Hub	Die Anleitung auf der Seite Konfiguration von Mitgliedskonten in einer AWS Organisation verwalten wurde verbessert.	7. Juli 2026
Dokumentation zur Netzwerkscanfunktion hinzugefügt	Dokumentation für die Netzwerkscanfunktion von Security Hub hinzugefügt	7. Juli 2026
KI-Inventar	Das KI-Inventar wurde hinzugefügt, das eine einheitliche Ansicht der verwalteten und selbst gehosteten Ressourcen für künstliche Intelligenz (KI) und maschinelles Lernen (ML) in Ihrer gesamten AWS Umgebung bietet. Weitere Informationen finden Sie unter KI-Inventar in AWS Security Hub.	7. Juli 2026

Aktualisierungen einer verwalteten Richtlinie — AWSSecurityHubV2ServiceRolePolicy	Security Hub hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert`AWSSecurityHubV2ServiceRolePolicy` . Durch die Updates wurden Berechtigungen zur Unterstützung von Integrationen von Drittanbietern hinzugefügt, einschließlich der Verwaltung von Konfigurationsrekordern von Drittanbietern, der Erstellung und Verwaltung von Konnektoren und des Abrufs von Web-Identitätstoken für den Verbund.	30. Juni 2026
Aktualisierungen einer verwalteten Richtlinie — AWSSecurityHubServiceRolePolicy	Security Hub CSPM hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert. `AWSSecurityHubServiceRolePolicy` Durch die Updates wurden Berechtigungen zur Unterstützung von Integrationen von Drittanbietern hinzugefügt. Dazu gehören die Verwaltung von Konfigurationsrekordern von Drittanbietern und das Abrufen von Connector-Integritätskennzahlen.	30. Juni 2026

Neuer Sicherheitsstandard	Security Hub CSPM hat den AI Security Best Practices-Standard veröffentlicht. Dieser Standard bietet eine kuratierte Reihe von Kontrollen, mit denen erkannt wird, wenn die eingesetzten KI-Ressourcen nicht den bewährten Sicherheitsverfahren entsprechen.	30. Juni 2026
Neue Sicherheitskontrollen	Security Hub CSPM hat acht neue Kontrollen für den AI Security Best Practices -Standard veröffentlicht. Die neuen Steuerelemente sind: Bedrock.1, BedrockAgentCore.7, SageMaker.20, SageMaker.21, SageMaker .22SageMaker.23SageMaker .24, und. SageMaker.25	30. Juni 2026

Aktualisierung der Expositionsergebnisse zu Art und Schweregrad der Wirkungsmerkmale	Zu den Expositionsergebnissen wurde der Merkmalstyp Wirkung hinzugefügt. Die Auswirkung beschreibt den potenziellen Explosionsradius, wenn eine Ressource gefährdet wird, und zwar auf der Grundlage der effektiven Genehmigungen der zugehörigen AWS Identity and Access Management Auftraggeber. Die Berechnung des Schweregrads wurde aktualisiert und verwendet nun eine Wahrscheinlichkeits- und Auswirkungs-Risikomatrix, die den NIST-Leitlinien entspricht. Es wurden Hinweise zur Problembehebung pro Ressource für Eigenschaften des Zugriffspfads hinzugefügt.	23. Juni 2026
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die ECS.1 und die RDS.18 Kontrollen entfernt und sie aus allen geltenden Standards entfernt. Seit der Einstellung von Amazon EC2-Classic Networking können Amazon Relational Database Service (Amazon RDS) -Instances nicht mehr außerhalb einer VPC bereitgestellt werden.	5. Juni 2026

Updates für den serviceverknüpften CSPM-Rekorder	Es wurden Informationen zum neuen serviceverknüpften Konfigurationsrekorder hinzugefügt, der es Security Hub CSPM ermöglicht, Sicherheitskontrollen auf der Grundlage von Informationen zur Ressourcenkonfiguration durchzuführen.	27. Mai 2026
Ergebnisse des ungenutzten Zugriffs	Security Hub hat Funktionen zum Generieren und Anzeigen ungenutzter Zugriffsergebnisse aus IAM Access Analyzer hinzugefügt. Grundlegendes zu ungenutzten Zugriffsergebnissen in Security Hub	19. Mai 2026

Neue Sicherheitskontrollen	Security Hub CSPM hat fünf neue Kontrollen veröffentlicht. Einige der Kontrollen unterstützen den FSBP-Standard (AWS Foundational Security Best Practices). Die meisten Kontrollen unterstützen die Anforderungen von NIST SP 800-53 Rev. 5. • Für den AWS FSBP-Standard lauten die IDs für die entsprechenden Kontrollen: und. BedrockAgentCore.5 BedrockAgentCore.6 • Für NIST SP 800-53 Rev. 5 lauten die IDs für die entsprechenden Kontrollen: BedrockAgentCore.3, und. BedrockAgentCore.4 SageMaker.18	15. Mai 2026
Aktualisierungen einer verwalteten Richtlinie — AWSSecurityHubServiceRolePolicy	Security Hub CSPM hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert. AWSSecurityHubServiceRolePolicy Mit den Updates wurden Berechtigungen zur Verwaltung von serviceverknüpften Security Hub CSPM-Konfigurationsrekordern und zur Erstellung der dienstbezogenen Rolle hinzugefügt. AWS Config	29. April 2026

Neue Sicherheitskontrollen	Security Hub CSPM hat vier neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Steuerelemente sind: BedrockAgentCore.1 ,, und BedrockAgentCore.2. RDS.51SageMaker.19	22. April 2026
Neue Sicherheitskontrollen	Security Hub CSPM hat fünf neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Steuerelemente sind: APIGateway.11,, EC2.183, EKS.9und. SageMaker .16SageMaker.17	7. April 2026
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die AppSync.6 Kontrollen AppSync.1 und sie aus dem FSBP-Standard (AWS Foundational Security Best Practices) entfernt. AWS AppSync bietet jetzt Standardverschlüsselung für alle aktuellen und future API-Caches.	9. März 2026
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die ECS.1 Steuerung eingestellt und sie aus dem FSBP-Standard (AWS Foundational Security Best Practices) und dem NIST-Standard SP 800-53 Rev. 5 entfernt.	4. März 2026

Neue Sicherheitskontrollen	Security Hub CSPM hat elf neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Kontrollen sind: APIGateway.10,,, ELB.21ELB.22, RDS.50und. SageMaker.9SageMaker .10SageMaker.11SageMaker .12SageMaker.13SageMaker .14SageMaker.15	16. Februar 2026
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die MQ.3 Steuerung eingestellt und sie aus allen geltenden Standards entfernt. Wir haben die Kontrolle aufgrund der Amazon MQ MQ-Anforderungen für automatische Upgrades kleinerer Versionen eingestellt. Bisher galt diese Kontrolle für den Standard AWS Foundational Security Best Practices (FSBP), den StandardNIST SP 800-53 Rev. 5 und den Standard PCI DSS v4.0.1.	12. Januar 2026

Aktualisierungen der Dokumentation zum Kostenschätzer	Der Dokumentation zum Security Hub Hub-Kostenschätzer wurden Informationen darüber hinzugefügt, wie kontenübergreifender Zugriff gewährt werden kann, um Schätzungen für Konten außer dem Verwaltungskonto vorzunehmen.	12. Januar 2026
Neue Sicherheitskontrollen	Security Hub CSPM hat fünf neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Steuerelemente sind: CloudFormation.4,, CloudFront.17, ECS.19und. ECS.20ECS.21	6. Januar 2026
Aktualisierungen der Sicherheitsstandards und -kontrollen	Aufgrund der Amazon MQ MQ-Anforderungen für automatische Upgrades kleinerer Versionen planen wir, die geltenden Standards am 12. Januar 2026 außer Betrieb zu nehmen MQ.3 und die Kontrolle aus allen geltenden Standards zu entfernen. Derzeit gilt die Kontrolle für den Standard AWS Foundation Security Best Practices (FSBP), den StandardNIST SP 800-53 Rev. 5 und den Standard PCI DSS v4.0.1.	12. Dezember 2025

Aktualisierter Inhalt für Service-Managed Standard: AWS Control Tower	Aktualisierter Inhalt für Service-Managed Standard: AWS Control Tower bietet eine verbesserte Anleitung zum Erstellen, Anzeigen und Deaktivieren von AWS Control Tower Steuerelementen in der Standardversion.	8. Dezember 2025
Neue Sicherheitskontrollen	Security Hub CSPM hat sieben neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Steuerelemente sind: Cognito.4,, Cognito.5, Cognito.6EC2.182, CloudFormation.3und. ECS.18SES.3	8. Dezember 2025
Aktualisierter Inhalt für die allgemeine Verfügbarkeit von Security Hub	Inhalt zur Unterstützung der Version für allgemeine Verfügbarkeit von AWS Security Hub hinzugefügt	2. Dezember 2025
Aktualisierter Inhalt für Security Hub	Es wurden Inhalte für Trends und Regions-Aggregation hinzugefügt. Diese Änderungen unterstützen die Vorschauversion von Security Hub.	21. November 2025

Aktualisierungen einer verwalteten Richtlinie — AWSSecurityHubV2ServiceRolePolicy	Security Hub hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert AWSSecurityHubV2ServiceRolePolicy . Mit den Updates wurden Messfunktionen für Amazon Elastic Container Registry AWS Lambda CloudWatch, Amazon und AWS Identity and Access Management zur Unterstützung von Security Hub Hub-Funktionen hinzugefügt. Die Updates fügten auch Unterstützung für globale AWS Config Rekorder hinzu. Diese Änderungen unterstützen die Vorschauversion von Security Hub.	17. November 2025
Aktualisierungen einer verwalteten Richtlinie — AWSSecurityHubOrganizationsAccess	Security Hub hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert AWSSecurityHubOrganizationsAccess . Mit den Updates wurden Berechtigungen zur Beschreibung von Ressourcenrichtlinien hinzugefügt, die Security Hub Hub-Funktionen unterstützen. Diese Änderungen unterstützen die Vorschauversion von Security Hub.	17. November 2025

Aktualisierungen einer verwalteten Richtlinie — `AWSSecurityHubFullAccess`	Security Hub hat die AWS verwaltete Richtlinie mit dem Namen aktualisiert`AWSSecurityHubFullAccess` . Mit den Updates wurden Funktionen rund um die Verwaltung GuardDuty, Amazon Inspector und die Kontoverwaltung hinzugefügt, um die Funktionen von Security Hub zu unterstützen. Diese Änderungen unterstützen die Vorschauversion von Security Hub.	17. November 2025
Aktualisierungen der Sicherheitskontrollen	Wir haben den Schweregrad von 10 Security Hub CSPM-Kontrollen geändert: CloudFront.7 CloudTrail.5, ELB.7, GuardDuty.7, MQ.3,, Opensearch.10, RDS.7 ServiceCatalog.1 SNS.4, und. SQS.3 Eine Aufschlüsselung der Änderungen finden Sie im Änderungsprotokoll für Security Hub CSPM-Steuerelemente.	13. November 2025
Neue Sicherheitskontrollen	Security Hub CSPM hat sechs neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht. Die neuen Steuerelemente sind: Cognito.3,,, DMS.13EC2.181, RDS.43und. RDS.47RDS.48	28. Oktober 2025

Neuer Sicherheitsstandard	Security Hub CSPM bietet jetzt einen Sicherheitsstandard, der dem CIS AWS Foundations Benchmark v5.0.0 entspricht. Dieser neue Standard umfasst 40 bestehende Sicherheitskontrollen. Die Kontrollen führen automatisierte Prüfungen durch, bei denen bewertet wird, ob bestimmte Ressourcen einer Teilmenge der im Framework definierten Anforderungen entsprechen.	16. Oktober 2025
Neue Integration von Drittanbietern	Elasticist eine neue Drittanbieter-Integration, die Erkenntnisse von Security Hub CSPM erhalten kann.	3. Oktober 2025

Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die Redshift.9 und die RedshiftServerless .7 Kontrollen entfernt und sie aus allen geltenden Standards entfernt. Wir haben diese Kontrollen aufgrund von Amazon Redshift Redshift-Einschränkungen eingestellt, die eine effektive Behebung der `FAILED` Ergebnisse für die Kontrollen verhinderten. Bisher galten diese Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) und den Standard NIST SP 800-53 Rev. 5. Die Redshift.9 Kontrolle galt auch für den Service-Managed-Standard.AWS Control Tower	24. September 2025
Regionale Verfügbarkeit	Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Neuseeland) verfügbar. Eine vollständige Liste, AWS-Regionen wo Security Hub CSPM derzeit verfügbar ist, finden Sie unter AWS Security Hub Hub-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz	19. September 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat zwei neue Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) veröffentlicht: und. CloudFront.16RDS.46	3. September 2025
Regionale Verfügbarkeit	Der AWS Resource Tagging-Standard ist jetzt in den Regionen Asien-Pazifik (Thailand) und Mexiko (Zentral) verfügbar.	29. August 2025
Aktualisierungen der Sicherheitsstandards und -kontrollen	Aufgrund der Einschränkungen von Amazon Redshift planen wir, die Redshift.9 und RedshiftServerless.7 Kontrollen einzustellen und sie am 15. September 2025 aus allen geltenden Standards zu entfernen. Derzeit gelten diese Kontrollen für den Standard AWS Foundational Security Best Practices (FSBP) und den Standard NIST SP 800-53 Rev. 5. Die Redshift.9 Kontrolle gilt auch für den Service-Managed-Standard.AWS Control Tower	15. August 2025

Neues Objekt mit Ressourcendetails in der ASFF	Das AWS Security Finding Format (ASFF) enthält jetzt ein `CodeRepository` Ressourcenobjekt. Dieses Objekt enthält Details zu einem externen Code-Repository, das Sie mit AWS Ressourcen verbunden und Amazon Inspector so konfiguriert haben, dass es nach Sicherheitslücken sucht.	1. August 2025
Regionale Verfügbarkeit	Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Taipeh) verfügbar. Eine vollständige Liste, AWS-Regionen wo Security Hub CSPM derzeit verfügbar ist, finden Sie unter AWS Security Hub Hub-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz	23. Juli 2025
Neue Integration von Drittanbietern	Dynatraceist eine neue Drittanbieter-Integration, die Erkenntnisse von Security Hub CSPM erhalten kann.	18. Juli 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat 13 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den FSBP-Standard (AWS Foundational Security Best Practices). Einige der Steuerungen unterstützen die Anforderungen von NIST SP 800-53 Rev. 5. • Für den AWS FSBP-Standard lauten die IDs für die entsprechenden Kontrollen: CloudFront.15, Cognito.2, EC2.180,, ELB.18, MSK.4, MSK.5, MSK.6RDS.45Redshift.18, S3.25und. SSM.6SSM.7 • Für NIST SP 800-53 Rev. 5 lauten die IDs für die entsprechenden Kontrollen: und. Lambda.7RDS.45	15. Juli 2025

Aktualisierungen bei der Generierung von Kontrollergebnissen	Um Ihnen die Nachverfolgung von Compliance-Änderungen zu erleichtern, aktualisiert Security Hub CSPM jetzt bestehende Kontrollergebnisse, anstatt neue Ergebnisse zu generieren, wenn sich der Compliance-Status einzelner Ressourcen ändert. Das bedeutet, dass Sie anhand der Daten einzelner Ergebnisse die Compliance-Änderungen für bestimmte Ressourcen anhand bestimmter Kontrollen verfolgen können.	3. Juli 2025
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die IAM.13Steuerung aus dem PCI DSS v4.0.1-Standard entfernt. Wir haben das IAM.17Steuerelement auch aus dem Standard NIST SP 800-171 Revision 2 entfernt. Die Standards schreiben die Prüfungen, die diese Kontrollen bieten, nicht ausdrücklich vor. Wir haben auch die zugehörigen Anforderungsdetails für diese Standards für bestimmte Kontrollen aktualisiert, mit denen die IAM-Passwortrichtlinien überprüft werden: IAM.7 und IAM.10 durch IAM.17.	30. Juni 2025

Aktualisierungen bei der Suche nach Aufbewahrungsfristen	Security Hub CSPM speichert archivierte Ergebnisse jetzt für 30 Tage statt für 90 Tage, wodurch die Anzahl der Ergebnisse reduziert werden kann. Für eine längerfristige Aufbewahrung können Sie Ergebnisse in einen S3-Bucket exportieren, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden.	20. Juni 2025
Aktualisierungen vorhandener verwalteter Richtlinien	Security Hub CSPM hat der AWS verwalteten Richtlinie mit dem Namen eine neue Berechtigung hinzugefügt. `AWSSecurityHubOrganizationsAccess` Die Berechtigung ermöglicht es der Unternehmensleitung, Security Hub und Security Hub CSPM innerhalb einer Organisation zu aktivieren und zu verwalten. Security Hub CSPM fügte der AWS verwalteten Richtlinie mit dem Namen auch eine neue Berechtigung hinzu. `AWSSecurityHubFullAccess` Die Berechtigung ermöglicht es Principals, eine dienstbezogene Rolle für Security Hub zu erstellen.	18. Juni 2025

Öffentliche Vorschauversion und eine neue verwaltete Richtlinie für Security Hub	Öffentliche Vorschauversion von AWS Security Hub und das AWS Security Hub Hub-Benutzerhandbuch. Diese Version enthält eine neue AWS verwaltete Richtlinie,`AWSSecurityHubV2ServiceRolePolicy` . Die Richtlinie ermöglicht es Security Hub, AWS Config Regeln und Security Hub Hub-Ressourcen in der Organisation eines Kunden und im Namen des Kunden zu verwalten. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	17. Juni 2025
Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die IAM.10Steuerung aus dem PCI DSS v4.0.1-Standard entfernt. Dieses Steuerelement prüft, ob die Kontopasswortrichtlinien für IAM-Benutzer die Mindestanforderungen erfüllen, einschließlich einer Mindestkennwortlänge von 7 Zeichen. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Die IAM.10 Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten.	30. Mai 2025

Neuer Sicherheitsstandard	Security Hub CSPM bietet jetzt einen Sicherheitsstandard, der dem Cybersicherheits- und Compliance-Framework von NIST SP 800-171 Revision 2 entspricht. Dieser neue Standard umfasst mehr als 60 bestehende Sicherheitskontrollen. Die Kontrollen führen automatisierte Prüfungen durch, bei denen bestimmte AWS-Services Ressourcen im Hinblick auf die Einhaltung einer Teilmenge der im Framework definierten Anforderungen bewertet werden.	29. Mai 2025
Aktualisierungen der Sicherheitskontrollen	Security Hub CSPM hat die Veröffentlichung der folgenden Steuerung für alle rückgängig gemacht AWS-Regionen: [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden. Bisher unterstützte dieses Steuerelement den FSBP-Standard (AWS Foundational Security Best Practices).	8. Mai 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat 9 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den FSBP-Standard (AWS Foundational Security Best Practices). Einige der Steuerungen unterstützen die Anforderungen von NIST SP 800-53 Rev. 5. • Für den AWS FSBP-Standard lauten die IDs für die entsprechenden Kontrollen: DocumentDB.6,, RDS.44, RedshiftServerless.2RedshiftServerless.3RedshiftServerless.5RedshiftServerless.6, und RedshiftServerless.7 (später eingestellt). • Für NIST SP 800-53 Rev. 5 lauten die IDs für die entsprechenden Kontrollen: CloudTrail.10RedshiftServerless.4, und RedshiftServerless.7 (später eingestellt).	7. Mai 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat 24 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den Standard AWS Foundational Security Best Practices (FSBP) oder AWS Resource Tagging. Einige der Kontrollen unterstützen die Anforderungen von NIST SP 800-53 Rev. 5. • Für den AWS FSBP-Standard lauten die IDs für die entsprechenden Kontrollen: EC2.173,, und RDS.41. RDS.42SageMaker.8 • Für den AWS Resource Tagging-Standard lauten die IDs für die entsprechenden Steuerelemente: Amplify.1Amplify.2, Batch.4, DataSync.2, EC2.174, EC2.175, EC2.176, EC2.177, EC2.178, EC2.179,, Redshift.17, SageMaker.6, SageMaker.7, SSM.5, Transfer.4, Transfer.5Transfer.6 und. Transfer.7 • Für NIST SP 800-53 Rev. 5 lauten die IDs für die entsprechenden Kontrollen: und. ECS.17RDS.42	16. April 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat vier neue Kontrollen für den Standard AWS Foundational Security Best Practices veröffentlicht. Die Kontrollen sind: • the section called “[FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ” • the section called “[FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Bereitstellung konfiguriert sein Multi-AZ” • the section called “[FSx.5] FSx for Windows File Server Server-Dateisysteme sollten für Multi-AZ die Bereitstellung konfiguriert sein” • the section called “[RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden”	18. März 2025

Aktualisierungen der Sicherheitsstandards und -kontrollen	Wir haben die RDS.18 Sicherheitskontrolle (die später eingestellt wurde) aus dem Standard „Best Practices AWS für Grundsicherheit“ entfernt und die Überprüfung der Anforderungen von NIST SP 800-53 Rev. 5 automatisiert. Seit der Einstellung von Amazon EC2-Classic Networking können Amazon Relational Database Service (Amazon RDS) -Instances nicht mehr außerhalb einer VPC bereitgestellt werden.	7. März 2025
Aktualisierungen der Kontrollergebnisse	Security Hub CSPM generiert jetzt `WARNING` Ergebnisse für ein aktiviertes Steuerelement, wenn die Ressourcenaufzeichnung AWS Config für den Ressourcentyp, den das Steuerelement überprüft, nicht aktiviert ist. Dies kann Ihnen helfen, potenzielle Konfigurationslücken bei Ihren Sicherheitskontrollen zu identifizieren und zu beheben.	25. Februar 2025

Neue Sicherheitskontrollen	Security Hub CSPM hat 11 neue Kontrollen veröffentlicht. Die Kontrollen sind: • the section called “[Connect .2] Bei Connect Customer-Instanzen sollte die CloudWatch Protokollierung aktiviert sein” • the section called “[ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys” • the section called “[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherhei tsrichtlinien verwenden” • the section called “[Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue” • the section called “[GuardDu ty.11] GuardDuty Runtime Monitoring sollte aktiviert sein” • the section called “[GuardDu ty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein” • the section called “[GuardDu ty.13] GuardDuty EC2	24. Februar 2025

Runtime Monitoring sollte aktiviert sein”

- the section called “[Network Firewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein”
- the section called “[RDS.40] RDS für SQL Server-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen”
- the section called “[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen”
- the section called “[Transfer.3] Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein”

Neue Sicherheitskontrollen	Security Hub CSPM hat 37 neue Steuerelemente für den AWS Resource Tagging Standard veröffentlicht. Security Hub CSPM hat außerdem die folgenden neuen Steuerelemente veröffentlicht: • the section called “[EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden” • the section called “[EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden” • the section called “[SageMaker.5] SageMaker Bei Modellen sollte die Netzwerkisolierung aktiviert sein”	22. Januar 2025
Neue Sicherheitskontrolle	Die von Security Hub CSPM veröffentlichten EC2.172 EC2 VPC Block Public Access-Einstellungen sollten den Internet-Gateway-Verkehr blockieren.	15. Januar 2025

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. • the section called “[Cognito .1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein” • the section called “[RDS.38] RDS für PostgreSQL-DB-Instances sollte bei der Übertragung verschlüsselt werden” • the section called “[RDS.39] RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden” • the section called “[Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben”	17. Dezember 2024
Security Hub CSPM unterstützt PCI DSS v4.0.1	Security Hub CSPM unterstützt jetzt Version 4.0.1 des Payment Card Industry Data Security Standard (PCI DSS). Weitere Informationen zum Standard und den dafür geltenden Kontrollen finden Sie unter PCI DSS in Security Hub CSPM.	11. Dezember 2024

Security Hub CSPM erhält Ergebnisse zur GuardDuty Angriffssequenz	Security Hub CSPM erhält jetzt Ergebnisse zur Angriffssequenz von Amazon GuardDuty Extended Threat Detection. Einzelheiten zum Auffinden der Angriffssequenz sind im Erkennungsobjekt des AWS Security Finding Formats (ASFF) verfügbar.	01. Dezember 2024
Security Hub CSPM wird ab sofort unterstützt AWS-Region	Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Malaysia) verfügbar. Für einige Sicherheitskontrollen gelten regionale Einschränkungen. Eine Liste der Kontrollen, die in dieser Region nicht verfügbar sind, finden Sie unter Regionale Beschränkungen für Security Hub CSPM-Steuerelemente.	22. November 2024
Änderungen an Config.1	Security Hub CSPM erhöhte den Schweregrad der Config.1 Kontrolle von `MEDIUM` bis `CRITICAL` und fügte neue Statuscodes und Statusgründe für fehlgeschlagene Config.1 Ergebnisse hinzu. Weitere Informationen zu den Änderungen finden Sie im Eintrag vom 20. November 2024 im Änderungsprotokoll für Security Hub CSPM-Steuerelemente.	20. November 2024

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. Diese Kontrollen sind Teil von AWS Foundational Security Best Practices und NIST SP 800-53 Rev. 5 und bewerten, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen Schnittstellen-VPC-Endpunkt für eine OR-Ressource verfügt. AWS-Service AWS • the section called “[EC2.55] VPCs sollten mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden” • the section called “[EC2.56] VPCs sollten mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden” • the section called “[EC2.57] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden” • the section called “[EC2.58] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert werden”	15. November 2024

- the section called “[EC2.60] VPCs sollten mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. • [AppSync.1] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden • [AppSync.6] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden • the section called “[EC2.170] EC2-Startvorlagen sollten Instance Metadata Service Version 2 (IMDSv2) verwenden” • the section called “[EC2.171] Bei EC2-VPN-Verbindungen sollte die Protokollierung aktiviert sein” • the section called “[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden” • the section called “[KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein” • the section called “[SNS.4] Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen”	18. Oktober 2024

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. • the section called “[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen” • the section called “[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein” • the section called “[Kinesis.3] Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen” • the section called “[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden” • the section called “[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch” • the section called “[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch” • the section called “[S3.24] Bei Multi-Region S3-Zugangspunkten sollten die Einstellungen zum Blockiere	3. Oktober 2024

n des öffentlichen Zugriffs aktiviert sein”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. • the section called “[Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein” • the section called “[CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden” • the section called “Bei [DataSync.1] DataSync Aufgaben sollte die Protokollierung aktiviert sein” • the section called “[EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein” • Glue.2 (im Ruhestand) • the section called “[Glue.3] AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden” • the section called “[WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden” • the section called “[WorkSpaces.2] WorkSpaces Root-Volumes sollten im	30. August 2024

	Ruhezustand verschlüsselt werden”	
Neues Befundpanel	Das neue Ergebnisfenster auf der Security Hub CSPM-Konsole hilft Ihnen, schnell Maßnahmen zu ergreifen, Ressourcendetails und den Befundverlauf zu überprüfen und weitere relevante Informationen zu einem Ergebnis zu finden.	16. August 2024
Update zur Config.1 Steuerung	Das Config.1Steuerelement überprüft, ob AWS Config es aktiviert ist, verwendet die dienstbezogene Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM hat einen benutzerdefinierten Steuerparameter mit dem Namen hinzugefügt. `includeConfigServiceLinkedRoleCheck` Wenn Sie diesen Parameter auf setzen`false`, können Sie sich von der Überprüfung abmelden, ob die serviceverknüpfte AWS Config Rolle verwendet wird.	15. August 2024

Geben Sie eine Heimatregion ohne verknüpfte Regionen an	Sie können jetzt einen Suchaggregator erstellen und eine Heimatregion einrichten, ohne eine Region mit der Heimatregion AWS-Regionen zu verknüpfen. Auf diese Weise können Sie die zentrale Konfiguration aktivieren, ohne verknüpfte Regionen angeben zu müssen.	25. Juli 2024

Wählen Sie Steuerelemente aus, die in mehreren Regionen verfügbar sind	Die folgenden Steuerelemente sind jetzt zusätzlich verfügbar AWS-Regionen, darunter USA Ost (Nord-Virginia) und USA Ost (Ohio). • the section called “[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden” • the section called “[DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben” • the section called “[DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben” • the section called “[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein” • the section called “[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden” • the section called “[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim	15. Juli 2024

Start öffentliche IP-Adressen zuweisen”

- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- the section called “[FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden”
- the section called “[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch”
- [MQ.3] Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben
- the section called “[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben”
- the section called “[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen”
- the section called “[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein”

- the section called “[Service Catalog.1] Servicekatalog-Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation”
- the section called “[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein” • the section called “[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein” • the section called “[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein” • the section called “[GuardDuty.9] GuardDuty RDS-Schutz sollte aktiviert sein” • the section called “[GuardDuty.10] GuardDuty S3-Schutz sollte aktiviert sein” • the section called “[Inspector.1] Amazon Inspector EC2-Scannen sollte aktiviert sein” • the section called “[Inspector.2] Amazon Inspector ECR-Scannen sollte aktiviert sein” • the section called “[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein”	11. Juli 2024

- the section called “[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein”

Veröffentlichung von CIS AWS Foundations Benchmark v3.0.0	Security Hub CSPM hat den Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 veröffentlicht. Die Version enthält die folgenden neuen Steuerelemente sowie Zuordnungen zu mehreren vorhandenen Steuerelementen. • the section called “[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff ab Version 0.0.0 zulassen. 0/0 zu den Verwaltungsports des Remoteservers” • the section called “[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen” • the section called “[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden” • the section called “[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess” • the section called “[IAM.28] Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein”	13. Mai 2024

- the section called “[S3.22] S3-Buckets für allgemeine Zwecke sollten Schreiberereignisse auf Objektebene protokollieren”
- the section called “[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden” • the section called “[DMS.10] DMS-Endpunkte für Neptune-Datenbanken sollten die IAM-Autorisierung aktiviert haben” • the section called “[DMS.11] DMS-Endpunkte für MongoDB sollten einen Authentifizierungsmechanismus aktiviert haben” • the section called “[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein” • the section called “[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden” • the section called “[EFS.6] EFS-Mount-Ziele sollten nicht mit Subnetzen verknüpft werden, die beim Start öffentliche IP-Adressen zuweisen”	3. Mai 2024

- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- the section called “[FSx.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden”
- the section called “[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch”
- [MQ.3] Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben
- the section called “[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben”
- the section called “[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen”
- the section called “[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein”
- the section called “[Service Catalog.1] Servicekatalog-

	Portfolios sollten innerhalb eines gemeinsam genutzt werden AWS nur Organisation” • the section called “[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden”	
AWS Standard für die Kennzeichnung von Ressourcen	Der AWS Resource Tagging Standard von Security Hub CSPM ist jetzt allgemein verfügbar, zusammen mit neuen Kontrollen, die für den Standard gelten.	30. April 2024
Aktualisierung der bestehenden verwalteten Richtlinie	Security Hub CSPM hat die AWS verwaltete Richtlinie mit dem Namen aktualisiertAmazonSecurityHubFullAccess , um Preisdetails für AWS-Services und Produkte abzurufen.	24. April 2024
In-context Konfiguration der Steuerparameter	Wenn Sie die zentrale Konfiguration verwenden, können Sie Steuerparameter jetzt kontextbezogen auf der Detailseite eines Steuerelements auf der Security Hub CSPM-Konsole konfigurieren.	29. März 2024

Aktualisieren Sie die bestehende verwaltete Richtlinie	Security Hub CSPM hat die AWS verwaltete Richtlinie aktualisiert, `AWSSecurityHubReadOnlyAccess` indem sie ein Feld hinzugefügt hat`Sid`.	22. Februar 2024
Neue Sicherheitskontrolle	Das Steuerelement [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein, ist jetzt verfügbar. Informationen zu regionalen Beschränkungen für dieses Steuerelement finden Sie unter Verfügbarkeit von Steuerelementen nach Regionen.	19. Februar 2024
Security Hub CSPM in Kanada West (Calgary) verfügbar	Security Hub CSPM ist jetzt in Kanada West (Calgary) verfügbar. Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar , mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	20. Dezember 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden” • the section called “[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein” • the section called “[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein” • the section called “[EKS.8] Bei EKS-Clustern sollte die Audit-Protokollierung aktiviert sein” • the section called “[EMR.2] Die Einstellung Amazon EMR Block Public Access sollte aktiviert sein” • the section called “[FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden”	14. Dezember 2023

- the section called “[Macie.1] Amazon Macie sollte aktiviert sein”
- the section called “[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein”
- the section called “[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden”
- the section called “[Network Firewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden”
- the section called “[Network Firewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein”
- the section called “Auf [Opensearch.10] OpenSearch Domains sollte das neueste Softwareupdate installiert sein”
- the section called “[PCA.1] AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein”
- the section called “[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein”

	• the section called “[S3.20] Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein”	
Bereicherung finden	Security Hub CSPM hat die neuen Finding-Felder `AwsAccountName` `ApplicationArn` , und `ApplicationName` zum AWS Security Finding Format (ASFF) hinzugefügt.	27. November 2023
Verbesserungen am Übersichts-Dashboard	Sie können jetzt auf der Übersichtsseite der Security Hub CSPM-Konsole auf weitere Dashboard-Widgets zugreifen, Dashboard-Filtersätze speichern, um sich schnell auf bestimmte Sicherheitsprobleme zu konzentrieren, und das Dashboard-Layout anpassen.	27. November 2023
Zentrale Konfiguration	Die zentrale Konfiguration ist jetzt verfügbar. Mit der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Security Hub CSPM, Standards und Kontrollen für mehrere Organisationskonten, Organisationseinheiten (OUs) und Regionen konfigurieren.	27. November 2023

Aktualisierungen für verwaltete Richtlinie	Security Hub CSPM hat der `AWSSecurityHubServiceRolePolicy` verwaltet en Richtlinie neue Berechtig ungen hinzugefügt, die es Security Hub CSPM ermöglich en, anpassbare Eigenscha ften der Sicherheitskontrolle zu lesen und zu aktualisieren.	26. November 2023
Benutzerdefinierte Steuerung sparameter	Sie können jetzt Parameter werte für ausgewählte Security Hub CSPM-Steuerelemente anpassen. Dadurch können die Ergebnisse für eine bestimmte Kontrolle Ihren Geschäftsanforderungen und Sicherheitserwartungen besser entsprechen.	26. November 2023
Aktualisierungen der verwaltet en Richtlinien	Security Hub CSPM hat die Richtlinien aktualisiert `AWSSecurityHubFullAccess` und `AWSSecurityHubOrganizationsAccess` verwaltet, die es Ihnen ermöglichen, die Funktionen von Security Hub CSPM bzw. deren Integration zu nutzen. AWS Organizations	16. November 2023

Bestehende Sicherheitskontrollen wurden zum Standard hinzugefügt: Service-Managed AWS Control Tower	Die folgenden vorhandenen Security Hub CSPM-Steuerelemente wurden dem Service-Managed Standard hinzugefügt:. AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14. November 2023

Aktualisierungen für verwaltete Richtlinie	Security Hub CSPM hat der `AWSSecurityHubServiceRolePolicy` verwalteten Richtlinie eine neue Tagging-Berechtigung hinzugefügt, die es Security Hub CSPM ermöglicht, Ressourcen-Tags zu lesen, die sich auf Ergebnisse beziehen.	7. November 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[AppSync .5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden” • the section called “[DMS.6] Für DMS-Replikationsin stanzen sollte das automatis che Upgrade der Nebenvers ionen aktiviert sein” • the section called “[DMS.7] Bei DMS-Replikationsau fgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein” • the section called “[DMS.8] Bei DMS-Replikationsau fgaben für die Quelldate nbank sollte die Protokoll ierung aktiviert sein” • the section called “[DMS.9] DMS-Endpunkte sollten SSL verwenden” • the section called “[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein” • the section called “[DocumentDB.4] Amazon DocumentDB-Cluster sollten	10. Oktober 2023

Auditprotokolle in Logs veröffentlichen CloudWatch”

- the section called “[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein”
- the section called “[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen”
- the section called “[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden”
- the section called “[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein”
- the section called “[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden”
- the section called “[MQ.5] ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby”
- the section called “[MQ.6] RabbitMQ-Broker sollten

den Cluster-Bereitstellungsmodus verwenden”

- the section called “[Network Firewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein”
- the section called “[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen”
- the section called “[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversion aktiviert sein”
- the section called “[Route53.2] In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden”
- the section called “[WAF.12] AWS WAF Für Regeln sollten CloudWatch Metriken aktiviert sein”

Aktualisierungen für verwaltete Richtlinie	Security Hub CSPM hat der `AWSSecurityHubServiceRolePolicy` verwalteten Richtlinie neue Organisationsaktionen hinzugefügt, die es Security Hub CSPM ermöglichen, Konto- und Organisationseinheiteninformationen (OU) abzurufen. Wir haben auch neue Security Hub CSPM-Aktionen hinzugefügt, die es Security Hub CSPM ermöglichen, Dienstkonfigurationen, einschließlich Standards und Kontrollen, zu lesen und zu aktualisieren.	27. September 2023

Bestehende Sicherheitskontrollen wurden zum Standard hinzugefügt: Service-Managed AWS Control Tower	Die folgenden vorhandenen Security Hub CSPM-Steuerelemente wurden dem Service-Managed Standard hinzugefügt:. AWS Control Tower • [Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt sein • the section called “[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen” • the section called “[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch” • the section called “[Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein”	26. September 2023

- the section called “[Neptune .4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein”
- the section called “[Neptune .5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein”
- the section called “[Neptune .6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden”
- the section called “[Neptune .7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben”
- the section called “[Neptune .8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren”
- the section called “[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden”

Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse sind verfügbar in AWS GovCloud (US)	Die Ansicht der konsolidierten Kontrollen und die konsolidierten Kontrollergebnisse sind jetzt in der verfügbar AWS GovCloud (US) Region. Auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	6. September 2023
Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse in den Regionen China verfügbar	Die Ansicht der konsolidierten Kontrollen und die konsolidierten Kontrollergebnisse sind jetzt in den Regionen China verfügbar. Auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	28. August 2023

Security Hub CSPM in der Region Israel (Tel Aviv) verfügbar	Security Hub CSPM ist jetzt in Israel (Tel Aviv) verfügbar . Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	08. August 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • [Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt sein • the section called "[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden" • the section called "[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen" • the section called "[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden" • the section called "[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch" • the section called "[Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein" • the section called "[Neptune.4] Bei Neptune-DB-Cluster n sollte der Löschschutz aktiviert sein"	28. Juli 2023

	• the section called “[Neptune .5] Bei Neptune-DB-Cluster n sollten automatische Backups aktiviert sein” • the section called “[Neptune .6] Neptune DB-Cluste r-Snapshots sollten im Ruhezustand verschlüsselt werden” • the section called “[Neptune .7] Neptune-DB-Cluster sollten die IAM-Daten bankauthentifizierung aktiviert haben” • the section called “[Neptune .8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren” • the section called “[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden”	
Neue Operatoren für Kriterien für Automatisierungsregeln	Sie können jetzt die Vergleich soperatoren CONTAINS und NOT_CONTAINS für die Zuordnung von Automatis ierungsregeln und Zeichenke ttenkriterien verwenden.	25. Juli 2023

Automatisierungsregeln	Security Hub CSPM bietet jetzt Automatisierungsregeln, die Ergebnisse auf der Grundlage der von Ihnen angegebenen Kriterien automatisch aktualisieren.	13. Juni 2023
Neue Integration von Drittanbietern	Snykist eine neue Drittanbieter-Integration, die Ergebnisse an Security Hub CSPM sendet.	12. Juni 2023

Bestehende Sicherheitskontrollen wurden zum Service-Managed Standard hinzugefügt: AWS Control Tower	Die folgenden vorhandenen Security Hub CSPM-Steuerelemente wurden dem Service-Managed Standard hinzugefügt:. AWS Control Tower • the section called “[Account.1] Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto” • the section called “[APIGateway.8] API-Gateway-Routen sollten einen Autorisierungstyp angeben” • the section called “[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert werden” • the section called “[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein” • the section called “[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen” • the section called “[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden”	12. Juni 2023

- the section called “[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden”
- the section called “[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben”
- the section called “[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden” • the section called “[AppSync .2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben” • the section called “[CloudFr ont.13] CloudFront Distribut ionen sollten die Origin-Zu griffskontrolle verwenden” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch” • the section called “[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüs selt werden mit AWS KMS keys” • the section called “[StepFun ctions.1] Step Functions Functions-Zustands maschinen sollten die Protokollierung aktiviert haben”	6. Juni 2023

Security Hub CSPM im asiatisch-pazifischen Raum (Melbourne) verfügbar	Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Melbourne) verfügbar . Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	25. Mai 2023
Verlauf finden	Security Hub CSPM kann jetzt den Verlauf eines Fundes in den letzten 90 Tagen verfolgen.	4. Mai 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar: • the section called “[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein” • the section called “[ELB.16] Application Load Balancers sollten mit einem verknüpft sein AWS WAF Web-ACL” • the section called “[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[S3.15] Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein”	29. März 2023
Erweiterte Unterstützung für konsolidierte Kontrollergebnisse	Die automatisierte Sicherheitsreaktion auf AWS Version 2.0.0 unterstützt jetzt konsolidierte Kontrollergebnisse.	24. März 2023
Security Hub CSPM in neuer Version erhältlich AWS-Regionen	Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Hyderabad), Europa (Spanien) und Europa (Zürich) verfügbar. In diesen Regionen gibt es Beschränkungen, welche Kontrollen verfügbar sind.	21. März 2023

Aktualisierung der verwalteten Richtlinie	Security Hub CSPM hat eine bestehende Berechtigung in der `AWSSecurityHubServiceRolePolicy` verwalteten Richtlinie aktualisiert.	17. März 2023

Neue Sicherheitskontrollen für den NIST 800-53-Standard	Security Hub CSPM hat die folgenden Sicherheitskontrollen hinzugefügt, die für den NIST 800-53-Standard gelten: • the section called “[Account.2] AWS-Konten sollte Teil eines sein AWS Organizations Organisation” • the section called “Für [CloudWatch.15] CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein” • the section called “[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden” • the section called “[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein” • the section called “[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein” • the section called “[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden” • EC2.29 — EC2-Instances sollten in einer VPC gestartet werden (eingestellt)	03. März 2023

	• the section called “[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden” • the section called “[S3.14] Für S3-Allzweck-Bucket s sollte die Versionierung aktiviert sein” • the section called “[WAF.11] AWS WAF Die Web-ACL-P rotokollierung sollte aktiviert sein”	
Nationales Institut für Standards und Technologie (NIST) 800-53 Rev. 5	Security Hub CSPM unterstüt zt jetzt den Standard NIST 800-53 Rev. 5 mit mehr als 200 anwendbaren Sicherhei tskontrollen.	28. Februar 2023
Konsolidierte Kontrollen: Ergebnisse anzeigen und kontrollieren	Mit der Veröffentlichung der konsolidierten Kontrollansicht werden auf der Kontrollseite der Security Hub CSPM-Konsole all Ihre Kontrolle n standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrolle rgebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	23. Februar 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. Für einige Kontrollen gelten regionale Einschränkungen. • the section called “Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein” • the section called “[ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein” • the section called “[ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein” • the section called “[ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden” • the section called “[ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden” • the section called “[ElastiCache.6] ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten	16. Februar 2023

	Redis OSS AUTH aktiviert haben” • the section called “[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden”	
Neue ASFF-Felder	Security Hub CSPM hat das AWS Security Finding Format (ASFF) ProductFields.ArchivalReasons:0/ReasonCode um ProductFields.ArchivalReasons:0/Description und erweitert.	8. Februar 2023
Neue ASFF-Felder	Security Hub CSPM hat das AWS Security Finding Format (ASFF) Compliance.SecurityControlId um Compliance.AssociatedStandards und erweitert.	31. Januar 2023
Details zur Sicherheitslücke sind jetzt verfügbar	Sie können jetzt in der Security Hub CSPM-Konsole Details zu Sicherheitslücken für Ergebnisse sehen, die Amazon Inspector an Security Hub CSPM sendet.	14. Januar 2023
Security Hub CSPM ist im Mittleren Osten (VAE) verfügbar	Security Hub CSPM ist jetzt im Mittleren Osten (VAE) verfügbar. Für einige Kontrollen gelten regionale Beschränkungen.	12. Januar 2023

Integration von Drittanbietern mit hinzugefügt MetricStream	Security Hub CSPM unterstützt jetzt die Integration von Drittanbietern MetricStream in allen Regionen außer China und. AWS GovCloud (US)	11. Januar 2023
Das Limit für Unternehmenskonten wurde erhöht	Security Hub CSPM unterstützt jetzt bis zu 11.000 Mitgliedskonten für jedes Security Hub CSPM-Administratorkonto pro Region.	27. Dezember 2022
ElasticBeanstalk.3 wurde zurückgesetzt	Security Hub CSPM hat die Steuerung [ElasticBeanstalk.3] rückgängig gemacht, zu der Elastic Beanstalk in allen Regionen Logs CloudWatch vom FSBP-Standard streamen soll.	21. Dezember 2022
Security Hub CSPM fügt neue Sicherheitskontrollen hinzu	Neue Security Hub CSPM-Steuerelemente stehen Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. Für einige Kontrollen gelten regionale Einschränkungen.	15. Dezember 2022

Hinweise zu kommenden Funktionen	Security Hub CSPM plant die Veröffentlichung von zwei neuen Funktionen: konsolidierte Kontrollansicht und konsolidierte Kontrolle rgebnisse. Diese kommenden Funktionen können sich auf bestehende Workflows auswirken, die auf Feldern und Werten zur Kontrollsuche basieren.	9. Dezember 2022
Amazon Security Lake-Integration jetzt verfügbar	Security Lake lässt sich jetzt in Security Hub CSPM integrieren, indem es die Ergebnisse von Security Hub CSPM empfängt.	29. November 2022
Support für Service-Managed Standard: AWS Control Tower	Security Hub CSPM unterstützt einen neuen Sicherheitsstandard namens Service-Managed Standard:. AWS Control Tower AWS Control Tower verwaltet diesen Standard.	28. November 2022
CIS AWS Foundations Benchmark v1.4.0 jetzt in China Regionen verfügbar	Security Hub CSPM unterstützt jetzt den CIS AWS Foundations Benchmark v1.4.0 in den Regionen China.	18. November 2022
Die Cloud-Integration von Jira Service Management ist jetzt verfügbar	Jira Service Management Cloud erhält jetzt CSPM-Ergebnisse von Security Hub in allen verfügbaren Regionen, mit Ausnahme der Regionen China.	17. November 2022

AWS IoT Device Defender Integration jetzt verfügbar	AWS IoT Device Defender sendet jetzt Ergebnisse an Security Hub CSPM in allen verfügbaren Regionen.	17. November 2022
Support für CIS AWS Foundations Benchmark v1.4.0	Security Hub CSPM bietet jetzt Sicherheitskontrollen, die den CIS AWS Foundations Benchmark v1.4.0 unterstüt zen. Dieser Standard ist in allen verfügbaren Regionen mit Ausnahme der Regionen China verfügbar.	9. November 2022
Support für Security Hub CSPM-Ankündigungen in AWS GovCloud (US)	Sie können jetzt Security Hub CSPM-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) in () und AWS GovCloud AWS GovCloud (US-EastUS-West) abonnieren, um Benachric htigungen über Security Hub CSPM zu erhalten.	3. Oktober 2022
AWS Security Hub CSPM fügt eine neue Sicherheitskontrolle hinzu	Die neue Security Hub CSPM-Steuerung AutoScaling.9steht Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. Die Kontrollen können regionalen Einschränkungen unterliegen.	01. September 2022

Abonnieren Sie die CSPM-Ankündigungen von Security Hub	Sie können jetzt Security Hub CSPM-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) abonnieren, um Benachrichtigungen über Security Hub CSPM zu erhalten.	2p. August 2022
Regionserweiterung für regionsübergreifende Aggregation	Cross-Region Die Aggregation ist jetzt für Ergebnisse, Aktualisierungen und Einblicke in alle Bereiche verfügbar. AWS GovCloud (US)	2.August 2022
Neue Produktintegrationen von Drittanbietern	Fortinet — FortiCNP ist eine Drittanbieter-Integration, die Security Hub CSPM-Ergebnisse empfängt, und JFrog ist eine Drittanbieter-Integration, die Ergebnisse an Security Hub CSPM sendet.	26. Juli 2022
EC2.27 ist im Ruhestand	Security Hub CSPM wurde eingestellt EC2.27 — Beim Ausführen von EC2-Instances sollten keine Schlüsselpaare verwendet werden, eine frühere Kontrolle im Standard AWS Foundational Security Best Practices (FSBP).	20. Juli 2022

Lambda.2 unterstützt Python3.6 nicht mehr	Security Hub CSPM unterstützt Python3.6 nicht mehr als Parameter für Lambda.2 — Lambda-Funktionen sollten unterstützte Laufzeiten verwenden, ein Steuerelement im Standard AWS Foundational Security Best Practices (FSBP).	19. Juli 2022
AWS Security Hub CSPM fügt neue Sicherheitskontrollen hinzu	Neue Security Hub CSPM-Steuerelemente stehen Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. Für einige Kontrollen gelten regionale Einschränkungen.	22. Juni 2022
AWS Security Hub CSPM unterstützt eine neue Region	Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Jakarta) verfügbar. Einige Steuerelemente sind in dieser Region nicht verfügbar.	7. Juni 2022
Verbesserte Integration zwischen AWS Security Hub CSPM und AWS Config	Security Hub CSPM-Benutzer können die Ergebnisse der AWS Config Regelauswertungen als Ergebnisse in Security Hub CSPM sehen.	6. Juni 2022

Es wurde die Möglichkeit hinzugefügt, automatisch aktivierte Standards zu deaktivieren	Für Benutzer, die mit integriert sind AWS Organizations, ermöglicht diese Funktion, sich beim Security Hub CSPM-Administratorkonto anzumelden und neue Mitgliedskonten von den automatisch aktivierten Standards abzumelden.	25. April 2022
Erweiterte regionsübergreifende Aggregation	Es wurde eine regionsübergreifende Aggregation hinzugefügt, um Status und Sicherheitsbewertungen zu kontrollieren.	20. April 2022
CompanyName und ProductName sind jetzt Attribute der obersten Ebene	Es wurden neue Attribute der obersten Ebene hinzugefügt, um Firmen- und Produktnamen für benutzerdefinierte Integrationen festzulegen	1. April 2022
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden neue Kontrollen hinzugefügt	Der Standard „Best Practices “ von AWS Foundational Security wurde um 5 neue Kontrollen erweitert.	31. März 2022
ASFF wurde um neue Objekte mit Ressourcendetails erweitert	`AwsRdsDbSecurityGroup` Ressourcentyp zu ASFF hinzugefügt.	25. März 2022
Zusätzliche Ressourcendetails in ASFF hinzugefügt	Zusätzliche Details zu`AwsAutoScalingScalingGroup` , `AwsElbLoadBalancer` `AwsRedshiftCluster` , und `AwsCodeBuildProject` hinzugefügt.	25. März 2022

Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden neue Steuerelemente hinzugefügt	Der Standard „Best Practices “ von AWS Foundational Security wurde um 15 neue Kontrollen erweitert.	16. März 2022
Dem AWS Foundational Security Best Practices-Standard und dem Payment Card Industry Data Security Standard (PCI DSS) wurden neue Kontrollen hinzugefügt	Neue Steuerelemente für Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing und CloudFront zum Standard „Best Practices für AWS grundlegende Sicherheit“ hinzugefügt. Außerdem wurden dem PCI DSS zwei neue Steuerungen für OpenSearch Service hinzugefügt.	15. Februar 2022
ASFF wurde ein neues Feld hinzugefügt	Neues Feld hinzugefügt: Beispiel.	26. Januar 2022
Integration mit hinzugefügt AWS Health	AWS Health verwendet Service-to-Service-Ereignisnachrichten, um Ergebnisse an Security Hub CSPM zu senden.	19. Januar 2022
Integration mit hinzugefügt AWS Trusted Advisor	Trusted Advisor sendet die Ergebnisse seiner Prüfungen als Security Hub CSPM-Ergebnisse an Security Hub CSPM. Security Hub CSPM sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an. Trusted Advisor	18. Januar 2022

Objekte mit Ressourcendetails in ASFF wurden aktualisiert	`MixedInstancesPolicy` und `AvailabilityZones` wurden zu `AwsAutoScalingAutoScalingGroup` hinzugefügt. Hinzufügung von `MetadataOptions` zu `AwsAutoScalingLaunchConfiguration` . Hinzufügung von `BucketVersioningConfiguration` zu `AwsS3Bucket` .	20. Dezember 2021
Die Ausgabe für die ASFF-Dokumentation wurde aktualisiert	Die Beschreibungen der ASFF-Attribute waren zuvor in einem einzigen Thema zusammengefasst. Jedes Objekt der obersten Ebene und jedes Objekt mit Ressourcendetails befindet sich jetzt in einem eigenen Thema. Das Thema ASFF-Syntax enthält Links zu diesen Themen.	20. Dezember 2021
ASFF wurde um neue Objekte mit Ressourcendetails erweitert für AWS Network Firewall	For AWS Network Firewall hat die folgenden Objekte mit Ressourcendetails hinzugefügt: `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` , und`AwsNetworkFirewallRuleGroup` .	20. Dezember 2021

Unterstützung für die neue Version von Amazon Inspector hinzugefügt	Security Hub CSPM ist in die neue Version von Amazon Inspector sowie in Amazon Inspector Classic integrier t. Amazon Inspector sendet Ergebnisse an Security Hub CSPM.	29. November 2021
Der Schweregrad von wurde geändert EC2.19	Der Schweregrad von EC2.19 (Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen) wurde von Hoch auf Kritisch geändert.	17. November 2021
Neue Integration mit Sonrai Dig	Security Hub CSPM bietet jetzt eine Integration mit. Sonrai Dig Sonrai Digüberwacht Cloud-Umgebungen, um Sicherhei tsrisiken zu identifizieren. Sonrai Digsendet Ergebnisse an Security Hub CSPM.	12. November 2021
Aktualisierter Check für CIS 2.1 und CloudTrail.1 Kontrolle n	Zusätzlich zur Überprüfu ng, ob mindestens ein CloudTrail Multi-Region-Trail vorhanden ist, überprüft CIS 2.1 CloudTrail.1 jetzt auch, ob der `ExcludeManagementE ventSources` Parameter in mindestens einem der CloudTrail Multi-Region-Trails leer ist.	9. November 2021

Unterstützung für VPC-Endpunkte hinzugefügt	Security Hub CSPM ist jetzt in VPC-Endpunkte integriert AWS PrivateLink und unterstützt diese.	3. November 2021
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt	Neue Steuerelemente für Elastic Load Balancing (ELB.2 und ELB.8) und AWS Systems Manager (SSM.4) wurden hinzugefügt.	2. November 2021
Es wurden Ports zur Suche nach dem EC2.19 Steuerelement hinzugefügt	EC2.19 prüft jetzt auch, ob Sicherheitsgruppen keinen uneingeschränkten Eingangszugriff auf die folgenden Ports zulassen: 3000 (Go, und Ruby Web Development Frameworks) Node.js, 5000 (Python Web Development Frameworks), 8088 (Legacy-HTTP-Port) und 8888 (alternativer HTTP-Port)	27. Oktober 2021
Die Integration mit Cloud SIEM wurde hinzugefügt Logz.io	Logz.io ist ein Anbieter von Cloud-SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten ermöglicht, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren. Logz.io erhält Ergebnisse von Security Hub CSPM.	25. Oktober 2021

Unterstützung für die regionsübergreifende Aggregation von Ergebnissen hinzugefügt	Cross-Region Mithilfe der Aggregation können Sie alle Ihre Ergebnisse anzeigen, ohne die Regionen ändern zu müssen. Administratorkonten wählen eine Aggregationsregion und verknüpfte Regionen aus. Die Ergebnisse für das Administratorkonto und seine Mitgliedskonten werden von den verknüpften Regionen zur Aggregationsregion zusammengefasst.	20. Oktober 2021
Objekte mit Ressourcendetails in ASFF wurden aktualisiert	Details zum Viewer-Zertifikat wurden hinzugefügt. `AwsCloudFrontDistribution` Zusätzliche Details wurden hinzugefügt `AwsCodeBuildProject`. Load Balancer-Attribute wurden hinzugefügt zu `AwsElbV2LoadBalancer`. Die Konto-ID des S3-Bucket-Besitzers wurde hinzugefügt. `AwsS3Bucket`	8. Oktober 2021

Neue Objekte mit Ressourcendetails zu ASFF hinzugefügt	Die folgenden neuen Ressourcendetailobjekte wurden zu ASFF hinzugefügt:`AwsEc2VpcEndpointService` ,,`AwsEcrRepository` ,`AwsEksCluster` ,`AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` `AwsWafRegionalRateBasedRule` `AwsXrayEncryptionConfig`	8. Oktober 2021
Die veraltete Runtime wurde aus dem Steuerelement entfernt Lambda.2	Im Standard „Best Practices“ von AWS Foundation Security wurde die `dotnetcore2.1` Laufzeit aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.	6. Oktober 2021
Neuer Name für die Check Point-Integration	Die Integration mit Check Point Dome9 Arc heißt jetzt Check Point CloudGuard Posture Management. Der Integrations-ARN hat sich nicht geändert.	1. Oktober 2021
Die Integration mit Alcide wurde entfernt	Die Integration mit Alcide KAudit wurde eingestellt.	30. September 2021
Der Schweregrad von wurde geändert EC2.19	Der Schweregrad von [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen, wurde von Mittel auf Hoch geändert.	30. September 2021

Die Integration mit AWS Organizations wird jetzt in den Regionen China unterstützt	Die Security Hub CSPM-Integration mit Organizations wird jetzt in China (Peking) und China (Ningxia) unterstützt.	20. September 2021
Neue AWS Config Regel für die und Kontrollen S3.1 PCI.S3.6	Beides S3.1 und PCI.S3.6 stellen Sie sicher, dass die Amazon S3 S3-Einstellung Block Public Access aktiviert ist. Die AWS Config Regel für diese Steuerelemente wurde von `s3-account-level-public-access-blocks` auf geänderts`3-account-level-public-access-blocks-periodic` .	14. September 2021
Veraltete Laufzeiten wurden aus dem Steuerelement entfernt Lambda.2	Im Standard „Best Practices für AWS grundlegende Sicherheit“ wurden die `nodejs10.x` und `ruby2.5` Runtimes aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.	13. September 2021
Der Schweregrad der CIS 2.2-Steuerung wurde geändert	Im Benchmark-Standard der CIS AWS Foundations ist der Schweregrad für 2.2. — Stellen CloudTrail Sie sicher, dass die Validierung der Protokolldatei von Niedrig auf Mittel aktiviert ist.	13. September 2021

Aktualisiert ECS.1 Lambda.2, und entspricht dem SSM.1 Standard „Best Practices für AWS grundlegende Sicherheit“	Im Standard AWS Foundational Security Best Practices gibt es ECS.1 jetzt einen `SkipInactiveTaskDefinitions` Parameter, der auf gesetzt ist. `true` Dadurch wird sichergestellt, dass das Steuerelement nur aktive Aufgabendefinitionen überprüft. For Lambda.2, Python 3.9 zur Liste der Laufzeiten hinzugefügt. SSM.1 überprüft jetzt sowohl gestoppte als auch laufende Instanzen.	7. September 2021
PCI.Lambda.2 Die Steuerung schließt jetzt Lambda @Edge -Ressourcen aus	Im Payment Card Industry Data Security Standard (PCI DSS) -Standard schließt die PCI.Lambda.2 Steuerung nun Lambda @Edge -Ressourcen aus.	7. September 2021
Die Integration mit wurde hinzugefügt HackerOne Vulnerability Intelligence	Security Hub CSPM bietet jetzt eine Integration mit. HackerOne Vulnerability Intelligence Die Integration sendet die Ergebnisse an Security Hub CSPM.	7. September 2021

Objekte mit Ressourcendetails in ASFF wurden aktualisiert	FürAwsKmsKey , hinzugefügtKeyRotationStatus . FürAwsS3Bucket , hinzugefügt AccessControlList BucketLoggingConfiguration ,BucketNotificationConfiguration , undBucketWebsiteConfiguration .	2. September 2021
ASFF wurde um neue Objekte mit Ressourcendetails erweitert	ASFF wurde um die folgenden neuen Objekte mit Ressourcendetails erweitert: AwsAutoScalingLaunchConfiguration AwsEc2VpnConnection , und. AwsEcrContainerImage	2. September 2021
Dem Vulnerabilities Objekt in ASFF wurden Details hinzugefügt	InCvss, hinzugefügt Adjustments undSource. VulnerablePackages In wurden der Dateipfad und der Paketmanager hinzugefügt.	2. September 2021
Systems Manager Explorer und OpsCenter Integration werden jetzt in den Regionen China unterstützt	Der Security Hub ist CSPM-Integration mit SSM Explorer und OpsCenter wird jetzt in China (Peking) und China (Ningxia) unterstützt.	31. August 2021

Lambda.4 Die Kontrolle wird zurückgezogen	Security Hub CSPM stellt die Steuerung ein [Lambda.4] Für Lambda-Funktionen sollte eine Warteschlange mit unerlaubt en Briefen konfiguriert sein. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub CSPM führt keine Prüfungen daran durch.	31. August 2021
Das Steuerelement wird zurückgezogen PCI.EC2.3	Security Hub CSPM zieht die Steuerung zurück [PCI.EC2.3] Unbenutzte EC2-Sicherheitsgruppen sollten entfernt werden. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub CSPM führt keine Prüfungen daran durch.	27. August 2021
Änderung der Art und Weise, wie Security Hub CSPM Ergebnisse an benutzerd efinierte Aktionen sendet	Wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, sendet Security Hub CSPM jetzt jedes Ergebnis in einem separaten Security Hub Findings - Custom ActionEreignis.	20. August 2021

Ein neuer Code zur Begründung des Compliance-Status für benutzerdefinierte Lambda-Laufzeiten wurde hinzugefügt	Ein neuer Code für die Gründe für den `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` Compliance-Status wurde hinzugefügt. Dieser Ursachencode weist darauf hin, dass Security Hub CSPM keine Prüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen konnte.	20. August 2021
AWS Firewall Manager Integration wird jetzt in den Regionen China unterstützt	Die Security Hub CSPM-Integration mit Firewall Manager wird jetzt in China (Peking) und China (Ningxia) unterstützt.	19. August 2021
Neue Integrationen mit und Caveonix CloudForcepoint Cloud Security Gateway	Security Hub CSPM bietet jetzt Integrationen mit und. Caveonix Cloud Forcepoint Cloud Security Gateway Beide Integrationen senden die Ergebnisse an Security Hub CSPM.	10. August 2021

Neue Attribute `CompanyName` , und `Region` wurden zu `ProductName` ASFF hinzugefügt	`Region`Felder `CompanyName` `ProductName` , und wurden zur obersten Ebene der ASFF hinzugefügt. Diese Felder werden automatisch ausgefüllt und können, mit Ausnahme von benutzerdefinierten Produktintegrationen, nicht mit `BatchImportFindings` oder aktualisiert werden. `BatchUpdateFindings` Auf der Konsole werden beim Suchen nach Filtern diese neuen Felder verwendet. In der API verwenden die `ProductName` Filter `CompanyName` und die Attribute, die sich unter befinden`ProductFields` .	23. Juli 2021
Objekte mit Ressourcendetails in ASFF hinzugefügt und aktualisiert	Ein neuer `AwsRdsEventSubscription` Ressourcentyp und Ressourcendetails wurden hinzugefügt. Ressourcendetails für den `AwsEcsService` Ressourcentyp hinzugefügt. Dem Objekt mit den `AwsElasticsearchDomain` Ressourcendetails wurden Attribute hinzugefügt.	23. Juli 2021

Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 durch ES.8), Amazon RDS (RDS.16 durch RDS.23), Amazon Redshift (Redshift.4) und Amazon SQS () hinzugefügt. SQS.1	20. Juli 2021
Eine Berechtigung wurde innerhalb der mit dem Dienst verknüpften Richtlinie zur Verwaltung von Rollen verschoben	Die `config:PutEvaluations` Berechtigung wurde innerhalb der verwalteten Richtlinie verschoben `AWSSecurityHubServiceRolePolicy`, sodass sie auf alle Ressourcen angewendet wird.	14. Juli 2021
Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 und CloudFront.6), Amazon EC2 (EC2.17 und EC2.18), Amazon ECS (ECS.1), Amazon OpenSearch Service (ES.4), AWS Identity and Access Management (IAM.21), Amazon RDS (RDS.15) und Amazon S3 (S3.8) hinzugefügt.	8. Juli 2021

Es wurden neue Begründungscodes für den Compliance-Status für Kontrollergebnisse hinzugefügt	`INTERNAL_SERVICE_ERROR` weist darauf hin, dass ein unbekannter Fehler aufgetreten ist. `SNS_TOPIC_CROSS_ACCOUNT` gibt an, dass das SNS-Thema einem anderen Konto gehört. `SNS_TOPIC_INVALID` gibt an, dass das zugehörige SNS-Thema ungültig ist.	6. Juli 2021
Die Integration mit Amazon Q Developer in Chat-Anwendungen wurde hinzugefügt	Die Integration mit Amazon Q Developer in Chat-Anwendungen wurde hinzugefügt. Security Hub CSPM sendet Ergebnisse in Chat-Anwendungen an Amazon Q Developer.	30. Juni 2021
Der mit dem Dienst verknüpften, rollenverwalteten Richtlinie wurde eine neue Berechtigung hinzugefügt	Der verwalteten Richtlinie wurde eine neue Berechtigung hinzugefügt`AWSSecurityHubServiceRolePolicy` , damit die dienstbezogene Rolle Bewertungsergebnisse liefern kann. AWS Config	29. Juni 2021

Neue und aktualisierte Objekte mit Ressourcendetails im ASFF	Neue Ressourcendetailobjekte für ECS-Cluster und ECS-Aufgabendefinitionen hinzugefügt. Das EC2-Instance-Objekt wurde aktualisiert und listet nun die zugehörigen Netzwerkschnittstellen auf. Die Client-Zertifikat-ID für die API Gateway V2-Stufen wurde hinzugefügt. Die Lebenszykluskonfiguration für S3-Buckets wurde hinzugefügt.	24. Juni 2021
Die Berechnung der aggregierten Kontrollstatus und der Standardsicherheitsbewertungen wurde aktualisiert	Security Hub CSPM berechnet jetzt alle 24 Stunden den Gesamtkontrollstatus und die Standardsicherheitsbewertung. Bei Administratorkonten spiegelt die Bewertung nun wider, ob die einzelnen Kontrollen für jedes Konto aktiviert oder deaktiviert sind.	23. Juni 2021
Aktualisierte Informationen zum Umgang mit gesperrten Konten durch Security Hub CSPM	Es wurden Informationen darüber hinzugefügt, wie Security Hub CSPM mit Konten umgeht, die gesperrt wurden. AWS	23. Juni 2021

Es wurden Tabs hinzugefügt, um die aktivierten und deaktivierten Steuerelemente für das einzelne Administratorkonto anzuzeigen	Für das Administratorkonto enthalten die Hauptregister auf der Standarddetailseite aggregierte Informationen für alle Konten. Auf den neuen Registerkarten Aktiviert für dieses Konto und Deaktiviert für dieses Konto werden die Konten aufgeführt, die für das einzelne Administratorkonto aktiviert oder deaktiviert sind.	23. Juni 2021
Zu `java8.al2` den Parametern hinzugefügt für `Lambda.2`	Im Standard AWS Foundational Security Best Practices `java8.al2` zu den unterstützten Laufzeiten für das `Lambda.2` Steuerelement hinzugefügt.	8. Juni 2021
Neue Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator	Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator hinzugefügt. MicroFocus ArcSight erhält Ergebnisse von Security Hub CSPM. NETSCOUT Cyber Investigator sendet Ergebnisse an Security Hub CSPM.	7. Juni 2021
Details hinzugefügt für `AWSSecurityHubServiceRolePolicy`	Der Abschnitt mit verwalteten Richtlinien wurde aktualisiert, um Details für die bestehende verwaltete Richtlinie hinzuzufügen`AWSSecurityHubServiceRolePolicy` , die von der serviceverknüpften Rolle Security Hub CSPM verwendet wird.	4. Juni 2021

Neue Integration mit Jira Service Management	Der AWS Service Management Connector für Jira sendet Ergebnisse an Jira und verwendet sie, um Jira-Probleme zu erstellen. Wenn die Jira-Probleme aktualisiert werden, werden auch die entsprechenden Ergebnisse in Security Hub CSPM aktualisiert.	26. Mai 2021
Die Liste der unterstützten Kontrollen für die Region Asien-Pazifik (Osaka) wurde aktualisiert	Der Standard der CIS AWS Foundations und der Payment Card Industry Data Security Standard (PCI DSS) wurden aktualisiert, um auf die Kontrollen hinzuweisen, die im asiatisch-pazifischen Raum (Osaka) nicht unterstützt werden.	21. Mai 2021
Neue Integration mit Sysdig Secure für die Cloud	Es wurde eine Integration mit Sysdig Secure für die Cloud hinzugefügt. Die Integration sendet die Ergebnisse an Security Hub CSPM.	14. Mai 2021

Der Standard „Best Practices “ von AWS Foundational Security wurde um Kontrollen erweitert	Neue Steuerelemente für Amazon API Gateway (APIGateway.2 und APIGateway.3), AWS CloudTrail (CloudTrail.4 und CloudTrail.5), Amazon EC2 (EC2.15 und EC2.16), AWS Elastic Beanstalk (Elastic Beanstalk.1 und ElasticBe anstalk.2), AWS Lambda (Lambda.4), Amazon RDS (RDS.12— RDS.14), Amazon Redshift (Redshift.7), AWS Secrets Manager (SecretsM anager.3 und SecretsMa nager.4) und () hinzugefügt. AWS WAF WAF.1	10. Mai 2021
Aktualisierungen GuardDuty und Amazon RDS-Steue relemente	Der Schweregrad wurde von `GuardDuty.1` und `PCI.GuardDuty.1` von Mittel auf Hoch geändert. Ein `databaseEngines` Parameter wurde hinzugefü gt`RDS.8`.	4. Mai 2021
Dem ASFF wurden neue Ressourcendetails hinzugefügt	In `Resources.Details` wurden neue Ressource ndetailobjekte für Amazon EC2-Netzwerk-ACLs, Amazon EC2-Subnetze und Umgebungen hinzugefügt. AWS Elastic Beanstalk	3. Mai 2021

Konsolenfelder hinzugefügt, um Filterwerte für EventBridge Amazon-Regeln bereitzustellen	Die neuen vordefinierten Filtermuster für Security Hub EventBridge CSPM-Regeln bieten Konsolenfelder, mit denen Sie Filterwerte angeben können.	30. April 2021
Die Integration mit AWS Systems Manager Explorer wurde hinzugefügt und OpsCenter	Security Hub CSPM unterstützt jetzt eine Integration mit Systems Manager Explorer und. OpsCenter Die Integration erhält Ergebnisse von Security Hub CSPM und aktualisiert diese Ergebnisse in Security Hub CSPM.	26. April 2021
Neuer Typ für Produktintegrationen	Ein neuer Integrationstyp,`UPDATE_FINDINGS_IN_SECURITY_HUB`, weist darauf hin, dass eine Produktintegration die Ergebnisse aktualisiert, die sie von Security Hub CSPM erhält.	22. April 2021
„Hauptkonto“ wurde in „Administratorkonto“ geändert.	Der Begriff „Hauptkonto“ wird in „Administratorkonto“ geändert. Der Begriff wurde auch in der Security Hub CSPM-Konsole und API geändert.	22. April 2021

Aktualisiert APIGateway.1 , um HTTP durch Websocket zu ersetzen	Titel, Beschreibung und Problembehebung für wurden aktualisiert. APIGateway.1 Das Steuerelement sucht jetzt nach der Protokollierung der Websocket-API-Ausführung statt nach der Protokollierung der HTTP-API-Ausführung.	9. April 2021
GuardDuty Die Amazon-Integration wird jetzt in Peking und Ningxia unterstützt	Die CSPM-Integration mit Security Hub GuardDuty wird jetzt in den Regionen China (Peking) und China (Ningxia) unterstützt.	05. April 2021
Zu den unterstützten `nodejs14.x` Laufzeiten zur Steuerung hinzugefügt Lambda.2	Das Lambda.2 Steuerelement im Standard „Best Practices“ von Foundation Security unterstützt jetzt die `nodejs14.x` Laufzeit.	30. März 2021
Security Hub CSPM im asiatisch-pazifischen Raum (Osaka) eröffnet	Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar.	29. März 2021
Zu den Suchdetails wurden Felder für die Suche nach Anbietern hinzugefügt	Im Bereich „Ergebnisdetails“ enthält der neue Abschnitt „Felder für die Suche nach Anbietern“ die Werte für Zuverlässigkeit, Kritikalität, verwandte Ergebnisse, Schweregrad und Typen.	24. März 2021

Option hinzugefügt, um sensible Ergebnisse von Amazon Macie zu erhalten	Die Integration mit Macie kann jetzt so konfiguriert werden, dass sensible Ergebnisse an Security Hub CSPM gesendet werden.	23. März 2021
Umstellung auf die Kontoverwaltung AWS Organizations	Für Kunden, die bereits über ein Administratorkonto mit Mitgliedskonten verfügen, wurden neue Informationen hinzugefügt, wie sie von der Verwaltung von Konten auf Einladung zur Verwaltung von Konten mithilfe von Organizations wechseln können.	22. März 2021
Neue Objekte in ASFF für Informationen zur Konfiguration von Amazon S3 Public Access Block	In `Resources` bietet ein neues Objekt mit `AwsS3AccountPublicAccessBlock` Ressourcentyp und Details Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten. Im Objekt mit den `AwsS3Bucket` Ressourcendetails stellt das `PublicAccessBlockConfiguration` Objekt die Public Access Block-Konfiguration für den S3-Bucket bereit.	18. März 2021

Neues Objekt in ASFF, mit dem Anbieter gefunden werden können, um bestimmte Felder zu aktualisieren	Das neue `FindingProviderFields` Objekt in ASFF wird verwendet, `BatchImportFindings` um Werte für `Confidence` ,, `Criticality` `RelatedFindings` `Severity`, und bereitzustellen. `Types` Die ursprünglichen Felder sollten nur mit `BatchUpdateFindings` aktualisiert werden.	18. März 2021
Neues `DataClassification` Objekt für Ressourcen in ASFF	Das neue `Resources.DataClassification` Objekt in ASFF wird verwendet, um Informationen über sensible Daten bereitzustellen, die auf der Ressource erkannt wurden.	18. März 2021
`CONFIG_RETURNS_NOT_APPLICABLE` Mehrwert für die verfügbaren Compliance-Statuscodes	Für den `NOT_AVAILABLE` Konformitätsstatus wurde der Ursachencode entfernt `RESOURCE_NO_LONGER_EXISTS` und der Ursachencode hinzugefügt `CONFIG_RETURNS_NOT_APPLICABLE` .	16. März 2021

Neue verwaltete Richtlinie für die Integration mit AWS Organizations	Eine neue verwaltete Richtlinie,`AWSSecurityHubOrganizationsAccess` , gewährt den Organizations die Berechtigungen, die für das Organisationsverwaltungskonto und das delegierte Security Hub CSPM-Administratorkonto erforderlich sind.	15. März 2021
Informationen zu verwalteten Richtlinien und dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben	Die Informationen zu verwalteten Richtlinien wurden überarbeitet und erweitert . Sowohl die Informationen zu verwalteten Richtlinien als auch die Informationen zu dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben.	15. März 2021
Überarbeiteter Schweregrad für die Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14	Der Schweregrad der Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14 wurde auf Niedrig geändert.	3. März 2021
Das Steuerelement wurde entfernt RDS.11	Das RDS.11 Steuerelement wurde aus dem Standard „Best Practices für grundlegende Sicherheit“ entfernt.	3. März 2021
Die Integration für Turbot wurde aktualisiert	Die Turbot-Integration wurde aktualisiert, um sowohl Ergebnisse zu senden als auch zu empfangen.	26. Februar 2021

Dem Standard „Bewährte Methoden für grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 und EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 und ES.3), Elastic Load Balancing (ELB.6) und AWS Key Management Service (AWS KMS) (KMS.3) hinzugefügt.	11. Februar 2021
Optionaler `ProductArn` Filter zur API hinzugefügt `DescribeProducts`	Die `DescribeProducts` API-Operation enthält jetzt einen optionalen `ProductArn` Parameter. Der `ProductArn` Parameter wird verwendet, um die spezifische Produktintegration zu identifizieren, für die Details zurückgegeben werden sollen.	3. Februar 2021
Neue Integration mit Antivirus für Amazon S3 von Cloud Storage Security	Die Integration mit Antivirus for Amazon S3 sendet die Ergebnisse der Virensuche als Ergebnisse an Security Hub CSPM.	27. Januar 2021

Das Verfahren zur Berechnung der Sicherheitsbewertung für Administratorkonten wurde aktualisiert	Für ein Administratorkonto verwendet Security Hub CSPM einen separaten Prozess zur Berechnung der Sicherheitsbewertung. Das neue Verfahren stellt sicher, dass die Bewertung Kontrollen umfasst, die für Mitgliedskonten aktiviert, für das Administratorkonto jedoch deaktiviert sind.	21. Januar 2021
Neue Felder und Objekte im ASFF	Es wurde ein neues `Action` Objekt hinzugefügt, um Aktionen zu verfolgen, die gegen eine Ressource aufgetreten sind. Dem `AwsEc2NetworkInterface` Objekt wurden Felder hinzugefügt, um DNS-Namen und IP-Adressen zu verfolgen. Den Ressourcendetails wurde ein neues `AwsSsmPatchCompliance` Objekt hinzugefügt.	21. Januar 2021

Dem Standard „Best Practices für grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon CloudFront (CloudFront.1 durch CloudFront.4), Amazon DynamoDB (DynamoDB.1 durch DynamoDB.3), Elastic Load Balancing (ELB.3 durch ELB.5), Amazon RDS (RDS.9durch RDS.11), Amazon Redshift (Redshift.1 durch Redshift.3 und Redshift.6) und Amazon SNS () hinzugefügt. SNS.1	15. Januar 2021
Der Workflow-Status wird basierend auf dem Datensatzstatus oder dem Compliance-Status zurückgesetzt	Security Hub CSPM setzt den Workflow-Status automatisch von `NOTIFIED` oder `RESOLVED` auf zurück, `NEW` wenn ein archiviertes Ergebnis aktiviert wird oder wenn sich der Compliance-Status eines Befundes von entweder `PASSED` auf`FAILED`, `WARNING` oder ändert. `NOT_AVAILABLE` Diese Änderungen deuten darauf hin, dass zusätzliche Untersuchungen erforderlich sind.	7. Januar 2021
Es wurden `ProductFields` Informationen für Ergebnisse hinzugefügt, die auf Kontrollen basieren	Für Ergebnisse, die anhand von Kontrollen generiert wurden, wurden Informationen über den Inhalt des `ProductFields` Objekts im AWS Security Finding Format (ASFF) hinzugefügt.	29. Dezember 2020

Aktualisierungen von Managed Insights	Der Titel von Insight 5 wurde geändert. Es wurde ein neuer Insight (32) hinzugefügt, der nach IAM-Benutzern mit verdächtigen Aktivitäten sucht.	22. Dezember 2020
Aktualisierungen IAM.7 und Kontrollen Lambda.1	Im Standard „ AWS Fundation al Security Best Practices “ wurden die Parameter für IAM.7 aktualisiert. Der Titel und die Beschreibung von Lambda.1 wurden aktualisiert.	22. Dezember 2020
Erweiterte Integration mit ServiceNow ITSM	Die ServiceNow ITSM-Integration ermöglicht es Benutzern, automatisch Vorfälle oder Probleme zu erstellen, wenn ein Security Hub CSPM-Ergebnis eingeht. Aktualisierungen dieser Vorfälle oder Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub CSPM.	11. Dezember 2020
Neue Integration mit AWS Audit Manager	Security Hub CSPM bietet jetzt eine Integration mit AWS Audit Manager. Die Integration ermöglicht es Audit Manager, kontrollbasierte Ergebnisse von Security Hub CSPM zu erhalten.	08. Dezember 2020

Neue Integration mit Aqua Security Kube-bench	Security Hub CSPM hat eine Integration mit Aqua Security hinzugefügt. Kube-bench Die Integration sendet die Ergebnisse an Security Hub CSPM.	24. November 2020
Cloud Custodian ist jetzt in den Regionen China verfügbar	Die Integration mit Cloud Custodian ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.	24. November 2020
`BatchImportFindings` kann jetzt verwendet werden, um zusätzliche Felder zu aktualisieren	Bisher konnten Sie die `Types` Felder`Confidence`, `Criticality` `RelatedFindings` `Severity`, und nicht `BatchImportFindings` zum Aktualisieren verwenden. Wenn diese Felder nicht von aktualisiert wurden`BatchUpdateFindings`, können sie nun von aktualisiert werden`BatchImportFindings`. Sobald sie von aktualisiert wurden`BatchUpdateFindings`, können sie nicht mehr von aktualisiert werden`BatchImportFindings`.	24. November 2020

Security Hub CSPM ist jetzt integriert in AWS Organizations	Kunden können jetzt Mitgliedskonten mithilfe ihrer Organisationskontokonfiguration verwalten. Das Organisationsverwaltungskonto bestimmt das Security Hub CSPM-Administratorkonto, das festlegt, welche Organisationskonten in Security Hub CSPM aktiviert werden sollen. Der manuelle Einladungsprozess kann weiterhin für Konten verwendet werden, die nicht Teil einer Organisation sind.	23. November 2020
Das separate Suchlistenformat für Steuerelemente mit hohem Volumen wurde entfernt	Die Ergebnisliste für ein Steuerelement verwendet nicht mehr das Seitenformat „Ergebnisse“, wenn es eine sehr große Anzahl von Ergebnissen gibt.	19. November 2020
Neue und aktualisierte Integrationen von Drittanbietern	Security Hub CSPM unterstützt jetzt Integrationen mit cloudtamer.io, 3CoreSec, Prowler und Kubernetes Security. StackRox IBM QRadar sendet keine Ergebnisse mehr. Es empfängt nur Ergebnisse.	30. Oktober 2020

Option zum Herunterladen der Ergebnisliste von der Kontrolld etailseite hinzugefügt.	Auf der Seite mit den Kontrolld etails gibt es eine neue Download-Option, mit der Sie die Ergebnisliste in eine CSV-Datei herunterladen können. Die heruntergeladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie bestimmte Ergebnisse ausgewählt haben, enthält die heruntergeladene Liste nur diese Ergebnisse.	26. Oktober 2020
Option zum Herunterladen der Liste der Steuerelemente von der Standarddetailseite hinzugefügt.	Auf der Standarddetailseit e können Sie mit einer neuen Download-Option die Kontrollliste in eine CSV-Datei herunterladen. Die herunterg eladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie ein bestimmtes Steuerelement ausgewählt haben, enthält die heruntergeladene Liste nur dieses Steuerelement.	26. Oktober 2020

Neue und aktualisierte Partnerintegrationen	Security Hub CSPM ist jetzt integriert. ThreatModeler Die folgenden Partnerintegrationen wurden aktualisiert, um ihren neuen Produktnamen Rechnung zu tragen. Twistlock Enterprise Edition heißt jetzt Palo Alto Networks - Prisma Cloud Compute. Demisto, ebenfalls von Palo Alto Networks, ist jetzt Cortex XSOAR und Redlock ist jetzt Prisma Cloud Enterprise.	23. Oktober 2020
Security Hub CSPM in China (Peking) und China (Ningxia) eröffnet	Security Hub CSPM ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.	21. Oktober 2020
Überarbeitetes Format für ASFF-Attribute und Integrationen von Drittanbietern	Die Listen der ASFF-Attribute und Partnerintegrationen verwenden jetzt ein listenbasiertes Format anstelle von Tabellen. Die ASFF-Syntax, die Attribute und die Taxonomie der Typen sind jetzt in separaten Themen zusammengefasst.	15. Oktober 2020
Die Standard-Detailseite wurde neu gestaltet	Auf der Standarddetailseite für einen aktivierten Standard wird jetzt eine Liste mit Steuerelementen im Registerformat angezeigt. Die Registerkarten filtern die Kontrollliste auf der Grundlage des Kontrollstatus.	7. Oktober 2020

CloudWatch Ereignisse wurden ersetzt durch EventBridge	Verweise auf Amazon CloudWatch Events wurden durch Amazon ersetzt EventBridge.	1. Oktober 2020
Neue Integrationen mit Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks. VM-Series	Security Hub CSPM ist jetzt in Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks integriert. VM-Series Blue Hexagon for AWS und KAudit senden die Ergebnisse an Security Hub CSPM. VM-Series erhält Ergebnisse von Security Hub CSPM.	30. September 2020
Neue und aktualisierte Objekte mit Ressourcendetails in ASFF	Neue `Resources.Details` Objekte für`AwsApiGatewayRestApi` ,, `AwsApiGatewayStage` `AwsApiGatewayV2Api` ,`AwsApiGatewayV2Stage` , `AwsCertificateManagerCertificate` `AwsElbLoadBalancer` `AwsIamGroup` , und `AwsRedshiftCluster` hinzugefügt. Es wurden Details zu den `AwsIamAccessKey` Objekten`AwsCloudFrontDistribution` , `AwsIamRole` und hinzugefügt.	30. September 2020

Neues `ResourceRole` Attribut für Ressourcen in ASFF, um zu verfolgen, ob es sich bei einer Ressource um einen Akteur oder ein Ziel handelt.	Das `ResourceRole` Attribut für Ressourcen gibt an, ob es sich bei der Ressource um das Ziel der Suchaktivität oder um den Täter der Findungsaktivität handelt. Die gültigen Werte sind `ACTOR` und `TARGET`.	30. September 2020
AWS Systems Manager Patch Manager wurde zu den verfügbaren AWS Serviceintegrationen hinzugefügt	AWS Systems Manager Patch Manager ist jetzt in Security Hub CSPM integriert. Patch Manager sendet Ergebnisse an Security Hub CSPM, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.	22. September 2020
Der Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurde um neue Kontrollen erweitert	Neue Steuerelemente für die folgenden Dienste hinzugefügt: Amazon EC2 (EC2.7 und EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 durch RDS.8), Amazon S3 (S3.6) und AWS Secrets Manager (SecretsManager.1 und). SecretsManager.2	15. September 2020
Neue Kontextschlüssel für die IAM-Richtlinie zur Steuerung des Zugriffs auf Felder `BatchUpdateFindings`	IAM-Richtlinien können jetzt so konfiguriert werden, dass der Zugriff auf Felder und Feldwerte bei der Verwendung eingeschränkt wird. `BatchUpdateFindings`	10. September 2020

Erweiterter Zugriff auf `BatchUpdateFindings` für Mitgliedskonten	Standardmäßig haben Mitgliedskonten jetzt denselben Zugriff `BatchUpdateFindings` wie Administratorkonten.	10. September 2020
Neue Kontrollen AWS KMS im Foundational Security Best Practices Standard	Dem Foundational Security Best Practices Standard wurden zwei neue Kontrollen (KMS.1 und KMS.2) hinzugefügt. Mit den neuen Kontrollen wird geprüft, ob IAM-Richtlinien den Zugriff auf AWS KMS Entschlüsselungsaktionen einschränken.	9. September 2020
Die Ergebnisse für Kontrollen auf Kontoebene wurden entfernt	Security Hub CSPM generiert keine Ergebnisse mehr auf Kontoebene für eine Kontrolle. Es werden nur Ergebnisse auf Ressourcenebene generiert.	1. September 2020
Neues PatchSummary Objekt in ASFF	Das `PatchSummary` Objekt wurde der ASFF hinzugefügt. Das `PatchSummary` Objekt stellt Informationen zur Patch-Konformität einer Ressource im Verhältnis zu einem ausgewählten Konformitätsstandard bereit.	1. September 2020

Die Seite mit den Kontrolldetails wurde neu gestaltet	Die Detailseite für Steuerelemente wurde neu gestaltet. Die Liste mit den Ergebnissen von Kontrollen enthält Registerkarten, mit denen Sie die Liste schnell nach dem Konformitätsstatus filtern können. Sie können auch schnell unterdrückte Ergebnisse einsehen. Jeder Eintrag bietet Zugriff auf zusätzliche Details zur Suchressource, zur AWS Config Suchregel und zu Suchnotizen.	28. August 2020
Neue Filteroptionen für Ergebnisse	Für die Suche nach Filtern können Sie den Filter ist nicht verwenden, um Ergebnisse zu finden, bei denen ein Feldwert nicht dem Filterwert entspricht. Sie können den Befehl „Beginnt nicht mit“ verwenden, um nach Ergebnissen zu suchen, bei denen ein Feldwert nicht mit dem angegebenen Filterwert beginnt.	28. August 2020

Neue Objekte mit Ressourcendetails in ASFF	Neue `Resources.Details` Objekte für die folgenden Ressourcentypen hinzugefügt: `AwsDynamoDbTable` `AwsEc2Eip` ,,`AwsIamPolicy` ,`AwsIamUser` ,`AwsRdsDbCluster` ,`AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` `AwsSecretsManagerSecret`	18. August 2020
Neue Integration mit RSA Archer	Security Hub CSPM ist jetzt in RSA Archer integriert. RSA Archer erhält Ergebnisse von Security Hub CSPM.	18. August 2020
Neues Beschreibungsfeld für AwsKmsKey	Dem `AwsKmsKey` Objekt unter wurde ein `Description` Feld hinzugefügt`Resources.Details` .	18. August 2020
Es wurden Felder hinzugefügt zu AwsRdsDbInstance	Dem `AwsRdsDbInstance` Objekt unter wurden mehrere Attribute hinzugefügt`Resources.Details` .	18. August 2020

Die Art und Weise, wie Security Hub CSPM den Gesamtstatus einer Kontrolle bestimmt, wurde aktualisiert	Bei Kontrollen, für die keine Ergebnisse vorliegen, lautet der Status Keine Daten statt Unbekannt. Der Kontrollstatus umfasst sowohl Ergebnisse auf Konto- als auch auf Ressourcenebene. Der Kontrollstatus verwendet nicht den Workflow-Status von Ergebnissen, es sei denn, unterdrückte Ergebnisse werden ignoriert.	13. August 2020
Die Art und Weise, wie Security Hub CSPM die Sicherheitsbewertung für einen Standard berechnet, wurde aktualisiert	Bei der Berechnung der Sicherheitsbewertung für einen Standard ignoriert Security Hub CSPM jetzt Kontrollen mit dem Status Keine Daten. Die Sicherheitsbewertung ist das Verhältnis der bestandenen Kontrollen zu den aktivierten Kontrollen, ausgenommen Kontrollen ohne Daten.	13. August 2020
Neue Option zur automatischen Aktivierung neuer Kontrollen in aktivierten Standards	Es wurde eine Einstellungsoption hinzugefügt, um neue Steuerelemente in aktivierten Standards automatisch zu aktivieren. Sie können diese Option auch mithilfe der `UpdateSecurityHubConfiguration` API-Operation konfigurieren.	31. Juli 2020

Neue Kontrollen für den Payment Card Industry Data Security Standard (PCI DSS)	Dem PCI DSS-Standard wurden neue Steuerungen hinzugefügt. Die Bezeichner der neuen Steuerelemente PCI.DMS.1 lauten, PCI.EC2.5, PCI.EC2.6, PCI.ELBV2.1, PCI.GuardDuty.1, PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6 PCI.SageMaker.1 PCI.SSM.2, und. PCI.SSM.3	29. Juli 2020
Neue und aktualisierte Kontrollen für den Standard Foundational Security Best Practices	Dem Standard „Best Practices “ von Foundational Security wurden neue Kontrollen hinzugefügt. Die Kennungen der neuen Steuerelemente lauten AutoScaling.1,, DMS.1, EC2.4 EC2.6 S3.5, und. SSM.3 Der Titel von wurde aktualisiert ACM.1 und der Wert des `daysToExpiration` Parameters wurde auf 30 geändert.	29. Juli 2020
Neues `Vulnerabilities` Objekt in der ASFF	Das `Vulnerabilities` Objekt wurde hinzugefügt, das Informationen über Sicherheitslücken bereitstellt, die mit dem Befund in Verbindung stehen.	1. Juli 2020
Neue `Resource.Details` Objekte im ASFF für Auto Scaling Scaling-Gruppen, EC2-Volumes und EC2-VPCs	Die Objekte`AwsAutoScalingAutoScalingGroup` , und `AWSEc2Volume` wurden hinzugefügt. `AwsEc2Vpc` `Resource.Details`	1. Juli 2020

Neues `NetworkPath` Objekt in der ASFF	Das `NetworkPath` Objekt wurde hinzugefügt, das Informationen über einen Netzwerkpfad bereitstellt, der mit dem Ergebnis zusammenhängt.	1. Juli 2020
Ergebnisse automatisch auflösen, `Compliance.Status` wenn `PASSED`	Falls dies der Fall `Compliance.Status` ist`PASSED`, setzt `Workflow.Status` Security Hub CSPM bei Ergebnissen aus Kontrollen automatisch auf. `RESOLVED`	24. Juni 2020
AWS Command Line Interface Beispiele	AWS CLI Syntax und Beispiele für mehrere Security Hub CSPM-Aufgaben hinzugefügt. Beinhaltet die Aktivierung von Security Hub CSPM, die Verwaltung von Erkenntnissen, die Verwaltung von Standards und Kontrollen, die Verwaltung von Produktintegrationen und die Deaktivierung von Security Hub CSPM.	24. Juni 2020
Neues Attribut im ASFF `Severity.Original`	Das Attribut `Severity.Original` wurde hinzugefügt, wobei es sich um den ursprünglichen Schweregrad des Ergebnisanbieters handelt. Dies ersetzt das veraltete `Severity.Product` -Attribut.	20. Mai 2020

Neues `Compliance.StatusReasons` Objekt im ASFF für Details zum Status eines Steuerelements	Es wurde das Objekt `Compliance.StatusReasons` hinzugefügt, das zusätzlichen Kontext für den aktuellen Status einer Kontrolle bereitstellt.	20. Mai 2020
Neuer AWS grundlegender Standard für bewährte Sicherheitsverfahren	Der neue Standard „Bewährte Methoden für AWS grundlegende Sicherheitsverfahren“ wurde hinzugefügt. Dabei handelt es sich um eine Reihe von Kontrollen, die erkennen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.	22. April 2020
Neue Konsolenoption zum Aktualisieren des Workflow-Status für ein Ergebnis	Es wurden Informationen zur Verwendung der Security Hub-Konsole oder -API hinzugefügt, um den Workflow-Status für Ergebnisse festzulegen.	16. April 2020
Neue `BatchUpdateFindings` API für Kundenaktualisierungen von Ergebnissen	Es wurden Informationen zur Verwendung von `BatchUpdateFindings` hinzugefügt, um Informationen im Zusammenhang mit dem Prozess der Untersuchung eines Ergebnisses zu aktualisieren. `BatchUpdateFindings` ersetzt `UpdateFindings`, das veraltet ist.	16. April 2020

Aktualisierungen des AWS Security Finding Format (ASFF)	Mehrere neue Ressourcentypen hinzugefügt. Dem `Severity`-Objekt wurde ein neues `Label`-Attribut hinzugefügt. `Label` soll das `Normalized` -Feld ersetzen. Es wurde ein neues `Workflow`-Objekt hinzugefügt, um den Prozess einer Untersuchung zu einem Ergebnis zu verfolgen. `Workflow` enthält ein `Status`-Attribut, das das vorhandene `Workflowstate` -Attribut ersetzt.	12. März 2020
Aktualisierungen der Seite „Integrationen“	Aktualisiert, um die Änderungen an der Integrationsseite anzuzeigen. Für jede Integration zeigt die Seite nun die Integrationskategorie und ob jede Integration Ergebnisse an Security Hub CSPM sendet oder Ergebnisse von Security Hub CSPM empfängt. Sie enthält auch die spezifischen Schritte, die erforderlich sind, um jede Integration zu ermöglichen.	26. Februar 2020

Neue Integrationen von Drittanbieterprodukten	Die folgenden neuen Produktintegrationen wurden hinzugefügt: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security und Cognito Detect. Vectra.ai	21. Februar 2020
Neuer Sicherheitsstandard für den Payment Card Industry Data Security Standard (PCI DSS)	Der Security Hub CSPM-Sicherheitsstandard für den Payment Card Industry Data Security Standard (PCI DSS) wurde hinzugefügt. Wenn dieser Standard aktiviert ist, führt Security Hub CSPM automatisierte Prüfungen anhand von Kontrollen durch, die sich auf die PCI DSS-Anforderungen beziehen.	13. Februar 2020
Aktualisierungen des AWS Security Finding Format (ASFF)	Ein Feld für zugehörige Anforderungen für Standardkontrollen wurde hinzugefügt. Neue Ressourcentypen und neue Ressourcendetails wurden hinzugefügt. Mit dem ASFF können Sie jetzt bis zu 32 Ressourcen bereitstellen.	5. Februar 2020
Neue Option zum Deaktivieren einzelner Sicherheitsstandardkontrollen	Es wurden Informationen hinzugefügt, wie Sie steuern können, ob jedes einzelne Sicherheitsstandard-Steuerelement aktiviert ist.	15. Januar 2020

Aktualisierungen der Security Hub CSPM-Konzepte	Einige Beschreibungen wurden aktualisiert und den Security Hub CSPM-Konzepten neue Begriffe hinzugefügt.	21. September 2019
AWS Version für allgemeine Verfügbarkeit von Security Hub CSPM	Inhaltsaktualisierungen, um den Verbesserungen Rechnung zu tragen, die während der Betaphase an Security Hub CSPM vorgenommen wurden.	25. Juni 2019
Korrekturschritte für CIS AWS Foundations-Prüfungen hinzugefügt	Es wurden Korrekturschritte zu den in Security Hub CSPM unterstützten AWS Sicherheitsstandards hinzugefügt.	15. April 2019
Betaversion von AWS Security Hub CSPM	Die Beta-Version des AWS Security Hub CSPM-Benutzerhandbuchs wurde veröffentlicht.	18. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.